Reporting Strategies and Best Practices

Lab Tutorial Supplement

Table of Contents

LAB 1: Add Host Assets and Launch a Scan (Time: 10 mins)

NOTE
This lab tutorial includes steps for getting started with a scan job. These steps are covered in the **Vulnerability Management** and **Scanning Strategies and Best Practices** courses. You can directly skip to **Lab 2** if you are already familiar with these steps.

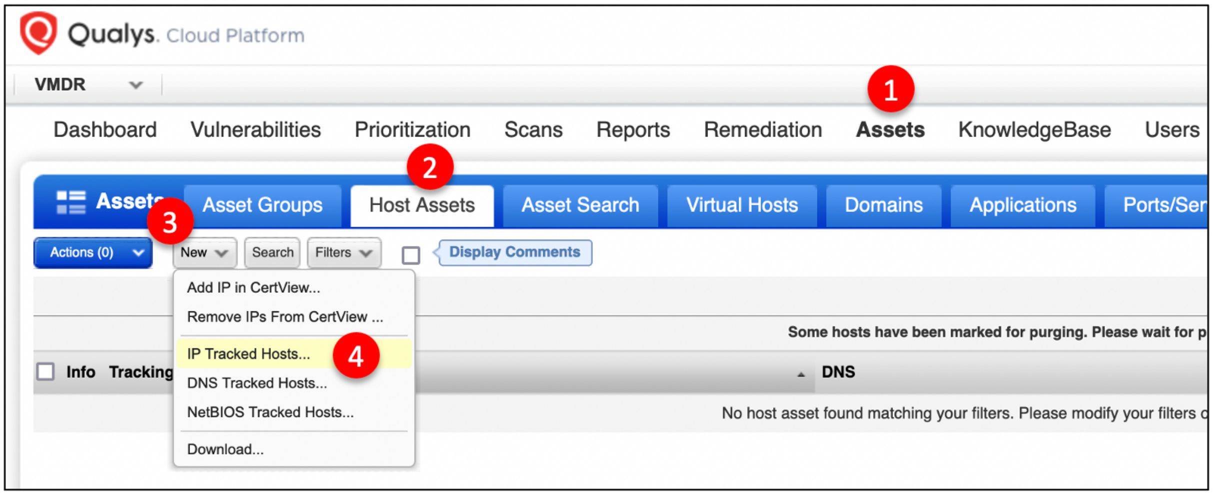
Add Host Assets

For scanning to begin, you must first add assets to your subscription. When adding host assets to your account, three basic methods are available for tracking discovered vulnerabilities:

- Host IP Address
- Host DNS Name
- Host NetBIOS Name

A fourth host tracking method, the Qualys Host ID, is used by default, for all "Cloud Agent" host assets. The Qualys Host ID is unique for each host asset, and is also available for "scannable" host assets, when the "Agentless Tracking" feature is enabled.

The steps in this tutorial will have you add host IPs to your subscription. These IP address "targets" will be used throughout the entire lab.

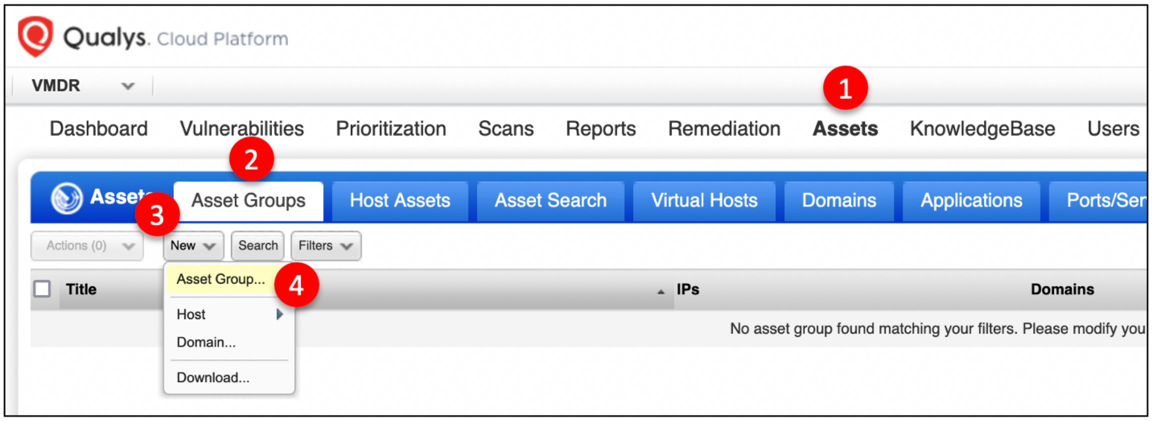


Some hosts have been marked for purging. Please wait for p

No host asset found matching your filters. Please modify your filters c

Create Asset Groups

Asset Groups and Asset Tags make excellent targets for your scans and reports. In this tutorial you will create one Asset Group for your Windows host assets and one for your Linux host assets.



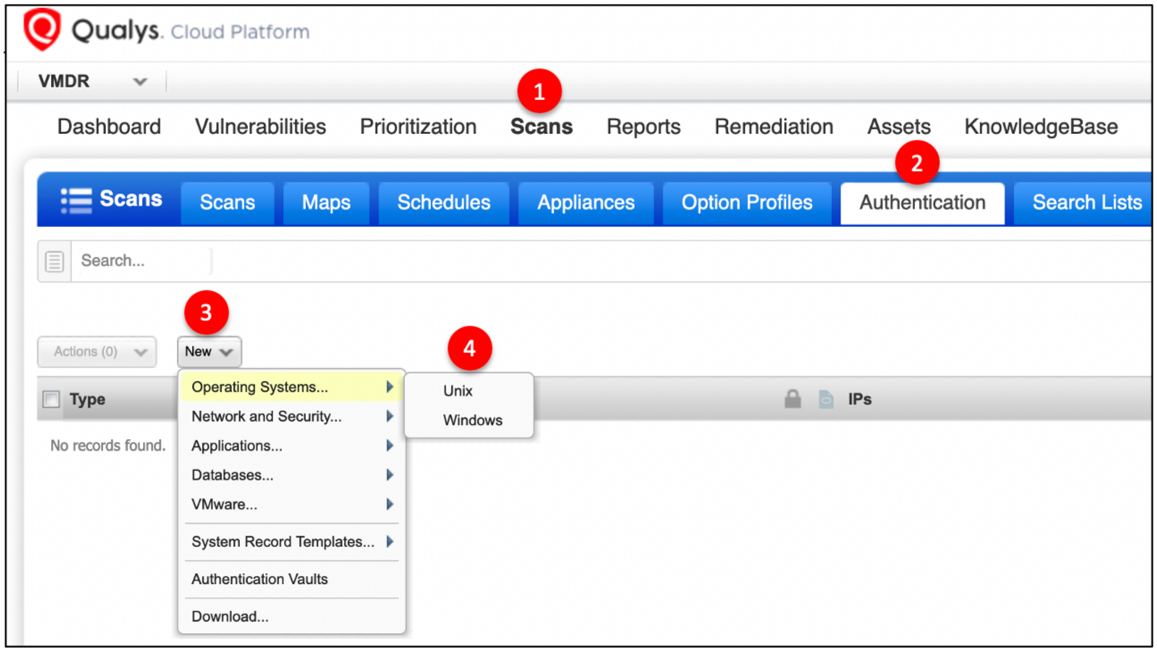
No asset group found matching your filters. Please modify you

The Qualys Platform automatically creates matching Asset Tags for each Asset Group added to your account. You'll find your matching Asset Tags in the AssetView application (embedded within the "Asset Groups" hierarchy).

Trusted Scanning

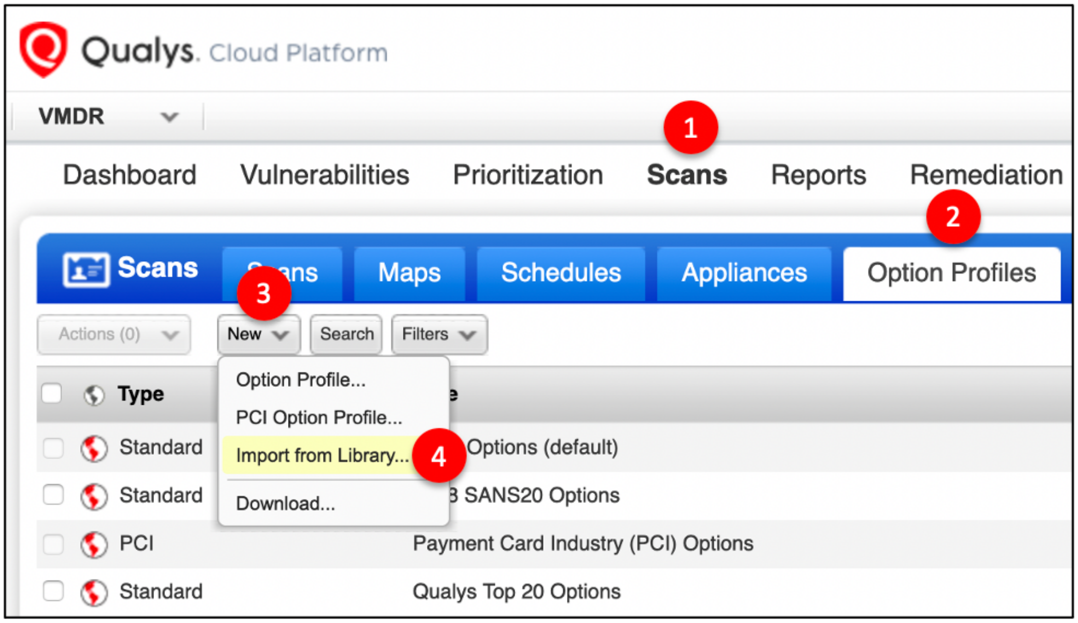
Qualys recommends performing vulnerability scans in "authenticated" mode or what we call "trusted" scanning. Performing a "trusted" scan requires one or more authentication records.

In this exercise, you'll create a Windows authentication record, a UNIX authentication record, and an Option Profile that uses them.



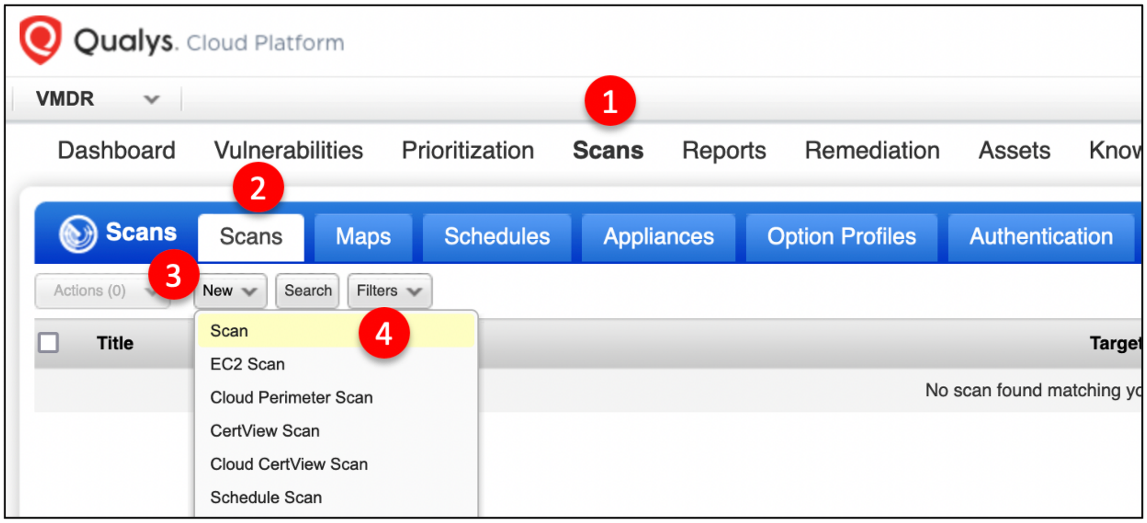
Import Option Profile

Authentication isn’t enabled by default and must be selected within an Option Profile. This exercise will import a pre-defined Option Profile that has Authentication enabled.

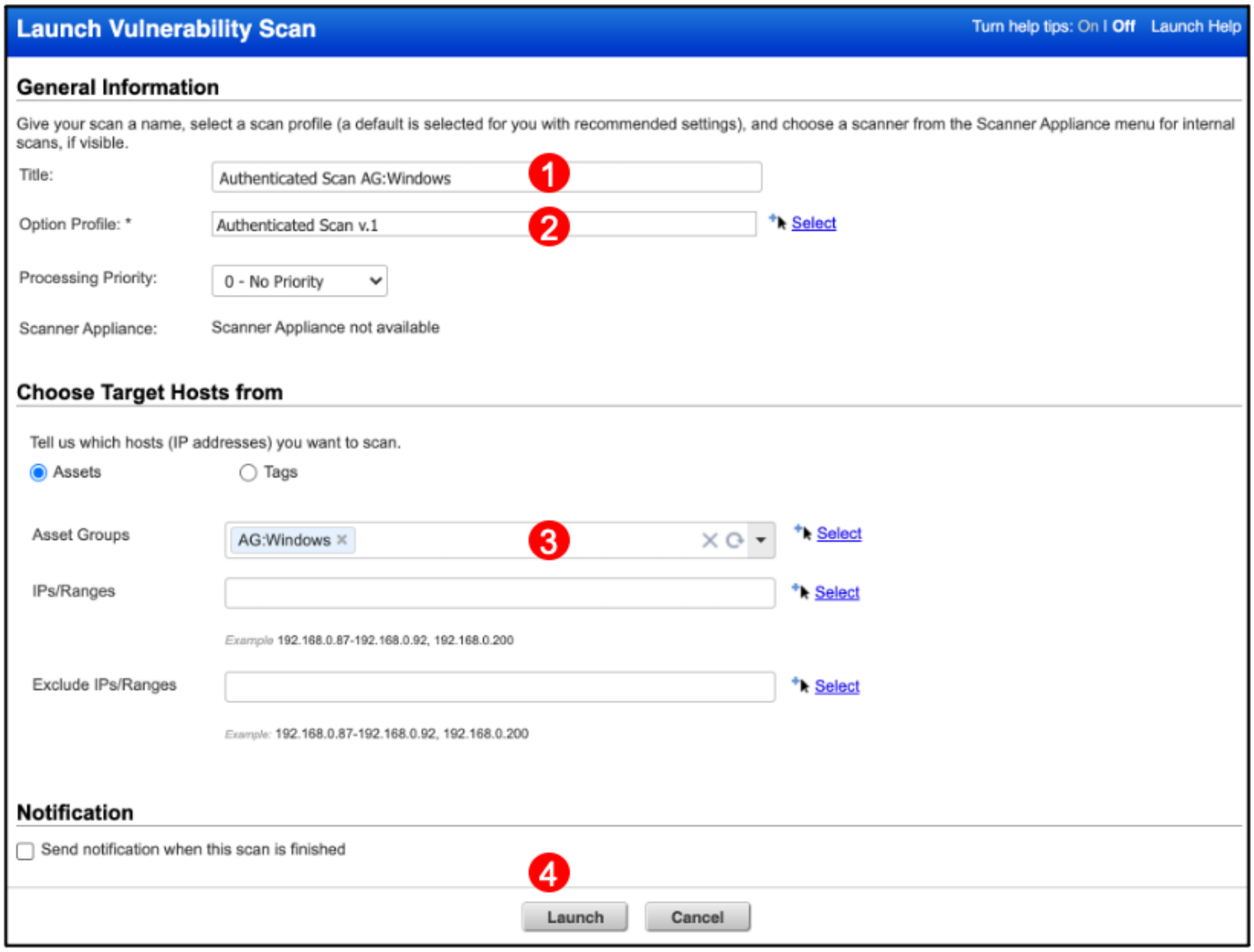


Launch Authenticated Scan

The exercise steps in this lab will use the Asset Groups and Option Profile you imported in the previous step. The steps are designed to collect assessment data, using the Qualys External Scanner Pool.



No scan found matching yo



Launch Vulnerability Scan
Turn help tips: On | Off Launch Help

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title:	Authenticated Scan AG:Windows (1)
Option Profile: *	Authenticated Scan v.1 (2) Select
Processing Priority:	0 - No Priority
Scanner Appliance:	Scanner Appliance not available

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

● Assets ○ Tags

Asset Groups	AG:Windows × (3) Select
IPs/Ranges	Select Example 192.168.0.87-192.168.0.92, 192.168.0.200
Exclude IPs/Ranges	Select Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Notification

□ Send notification when this scan is finished

(4)

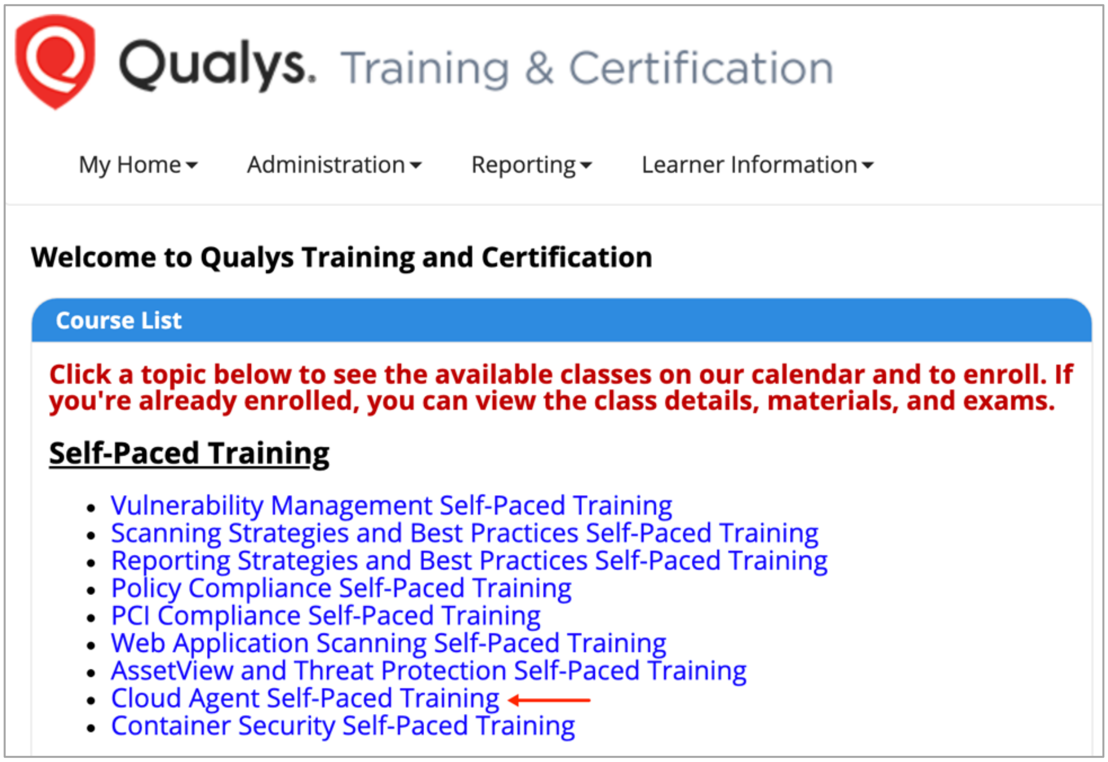
Navigate to the following URL to view the lab tutorial for this topic:

Lab: Add Host Assets and Launch a Scan Job

https://ior.ad/7Aty

Qualys Cloud Agent

For information on Cloud Agent installation and deployment, see the Qualys Cloud Agent Self-Paced training class (qualys.com/learning).



Welcome to Qualys Training and Certification

Course List

Click a topic below to see the available classes on our calendar and to enroll. If you're already enrolled, you can view the class details, materials, and exams.

Self-Paced Training

- Vulnerability Management Self-Paced Training
- Scanning Strategies and Best Practices Self-Paced Training
- Reporting Strategies and Best Practices Self-Paced Training
- Policy Compliance Self-Paced Training
- PCI Compliance Self-Paced Training
- Web Application Scanning Self-Paced Training
- AssetView and Threat Protection Self-Paced Training
- Cloud Agent Self-Paced Training
- Container Security Self-Paced Training

LAB 2: Analyze Impact of Configuration Changes (Time: 10 mins)

Technology and operational prerequisites change with time. As a result, IT infrastructure is constantly changing. These changes impact vulnerability tracking and reporting in different ways. Change to authentication settings, target ports and vulnerability detection criteria can all lead to data consistency issues. Vulnerabilities that are no longer targeted due to change in configuration settings will continue to remain open forever thus impacting remediation SLAs and also the overall reporting strategy.

In this activity, you will understand some of these scenarios in more detail.

Change in Authentication Mode

Majority of known vulnerabilities need authentication for detection. If a scan is unable to authenticate, these QID cannot be tested and will continue to retain its previous status. Reports that use host-based findings are influenced by changes in authentication mode (trusted vs. untrusted).

Example:

	Trusted Scan Findings	Host-based Report	Untrusted Scan Findings	Host-based Report
Host A	QID 100 ('A') QID 200 ('A') QID 300 🔑	QID 100 [NEW] QID 200 [NEW] QID 300 [NEW]	QID 100 ('A') QID 200 ('A')	QID 100 [ACTIVE] QID 200 [ACTIVE] QID 300 [NEW]

🔑 = authentication required ('A') = remote discovery (auth not required)

QID's that have the blue key icon on them are ones that need authentication for detection. If a scan is unable to authenticate, these QIDs cannot be tested and will continue to retain their previous status.

Navigate to the following URL to view the lab tutorials for this topic:

PLAY **Lab**: Analyse Impact of Change in Authentication Settings

https://ior.ad/7Avn

Change in Target Service Ports

Reports that use host-based findings are influenced by changes in the number and type of service ports targeted. If a port is not targeted on a scan, or cannot be tested for reasons like firewall filters, the QID associated with this port number will continue to retain its previous status.

Example:

	Standard Scan (1900 ports)	**Host-based Report**	**Light Scan (160 ports)**	**Host-based Report**
Host A	QID 700 `tcp/80` QID 800. `tcp/443` QID 900 `tcp/8443`	QID 700 [NEW] QID 800 [NEW] QID 900 [NEW]	QID 700 `tcp/80` QID 800 `tcp/443`	QID 700 [ACTIVE] QID 800 [ACTIVE] QID 900 [NEW]

The example shown here outlines the importance of targeting the required ports in a scan. The status of QID 900 will remain unchanged until another “Standard” scan is performed (or one that targets TCP port 8443).

Navigate to the following URL to view the lab tutorial for this topic:

PLAY **Lab**: Analyse Impact of Target Port Changes

https://ior.ad/7AyC

Change in Host “LIVE/DEAD” Status

Reports that use host-based findings are influenced by changes in host Live or Dead status. For a host to be tested for vulnerabilities, it should be found alive. The host alive checks used by Qualys can be configured under Scans > Option Profiles > Additional section.

Example:

	Live Host Scan Findings	Host-based Report	Dead Host Scan Findings	Host-based Report
Host A	QID 400 QID 500 QID 600	QID 400 [NEW] QID 500 [NEW] QID 600 [NEW]	Host Not Alive	QID 400 [NEW] QID 500 [NEW] QID 600 [NEW]

If a previously scanned host is found to be dead on the latest scan, the QID's detected earlier will continue to retain their status. The status of all QID's will remain unchanged, until another scan targeting these QID's finds the host as alive.

Note: There is no lab tutorial for this topic.

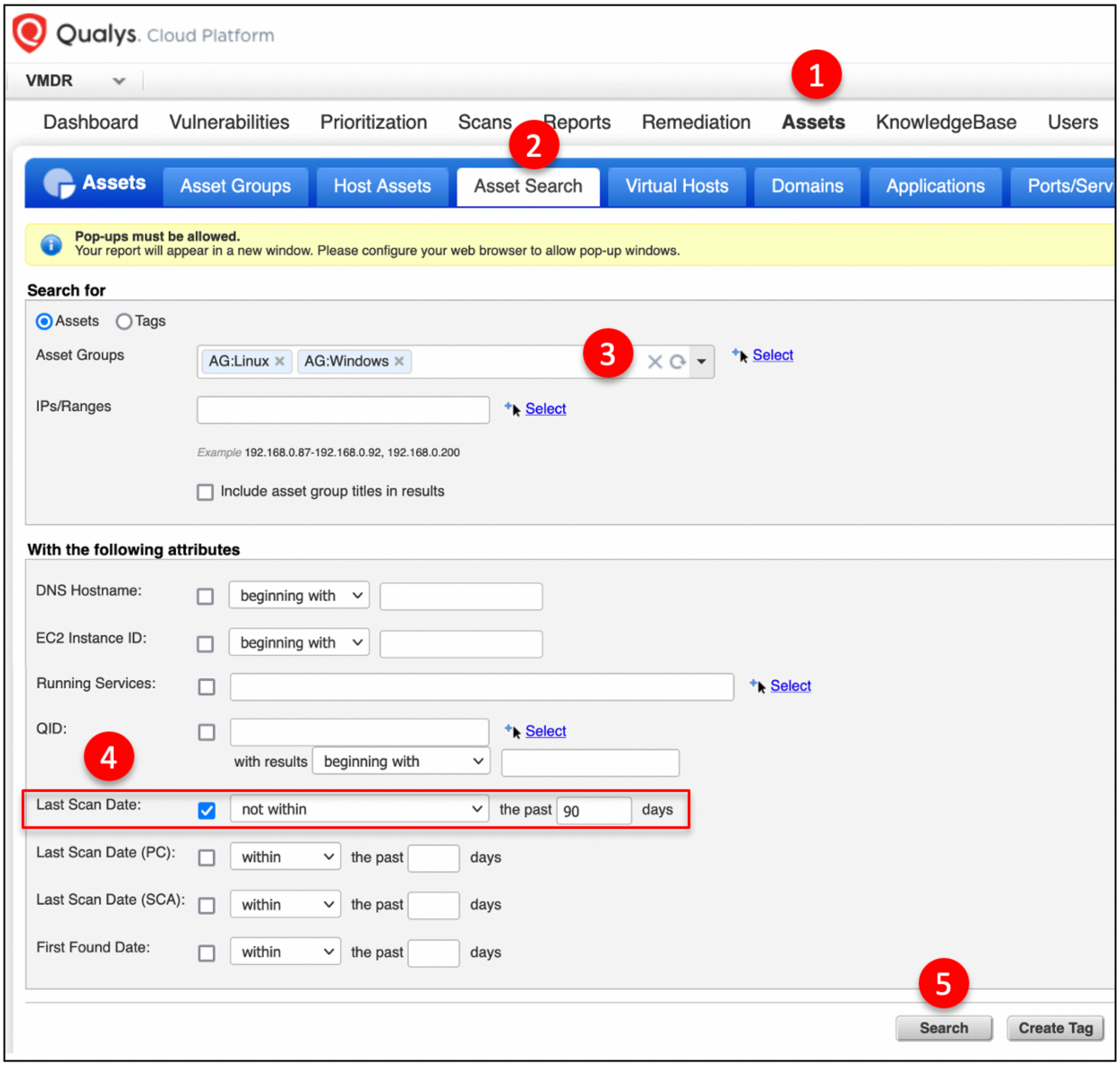
LAB 3: Purging and Removing Hosts (Time: 10 mins)

Purging a host is recommended when the host is being decommissioned or used in a completely new role – new operating system, new applications, new purpose. Purging becomes very important in highly dynamic and ephemeral environments where assets are replaced or deleted very frequently. Cloud provider environments are a good example. Removing a host is recommended when the IP is no longer needed to be scanned.

Identify Assets for Purging

It’s also essential to identify stale and inactive records for purging. There could be several criterial used to identify stale records. Common ones include assets that haven’t been scanned in X days, EC2 instances in a stopped/terminated state, inactive assets or assets that have been decommissioned, assets with authentication failures leading to missing and inconsistent vulnerability findings, etc.

You can search for assets meeting purging criteria using Asset Search in VM/VMDR.



Pop-ups must be allowed.
Your report will appear in a new window. Please configure your web browser to allow pop-up windows.

Search for

● Assets ○ Tags

Asset Groups: AG:Linux × AG:Windows ×

IPs/Ranges:

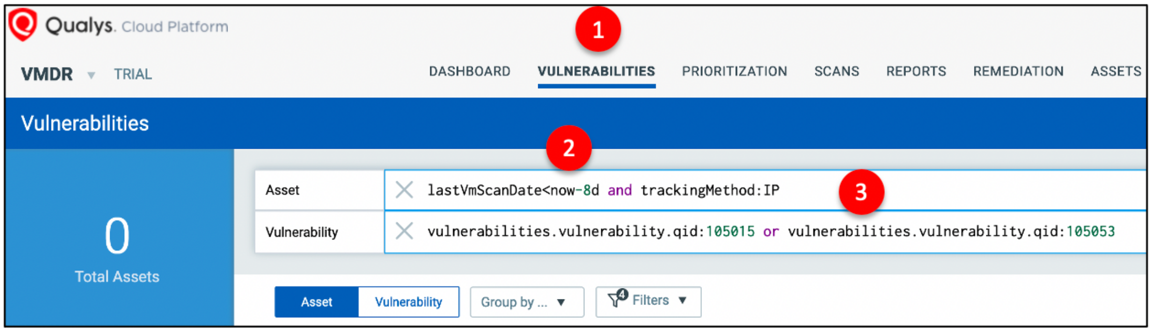
Example 192.168.0.87-192.168.0.92, 192.168.0.200

□ Include asset group titles in results

With the following attributes

DNS Hostname:	□	beginning with		
EC2 Instance ID:	□	beginning with		
Running Services:	□			
QID:	□	with results beginning with		
Last Scan Date:	☑	not within	the past 90	days
Last Scan Date (PC):	□	within	the past	days
Last Scan Date (SCA):	□	within	the past	days
First Found Date:	□	within	the past	days

You can also use QQL search queries to search for stale records. You can build widgets using QQL search queries to automatically identify assets for purging.



Asset: lastVmScanDate<now-8d and trackingMethod:IP

Vulnerability: vulnerabilities.vulnerability.qid:105015 or vulnerabilities.vulnerability.qid:105053

0 Total Assets

In the example above, the query will return any IP tracked assets if the following criteria is met:

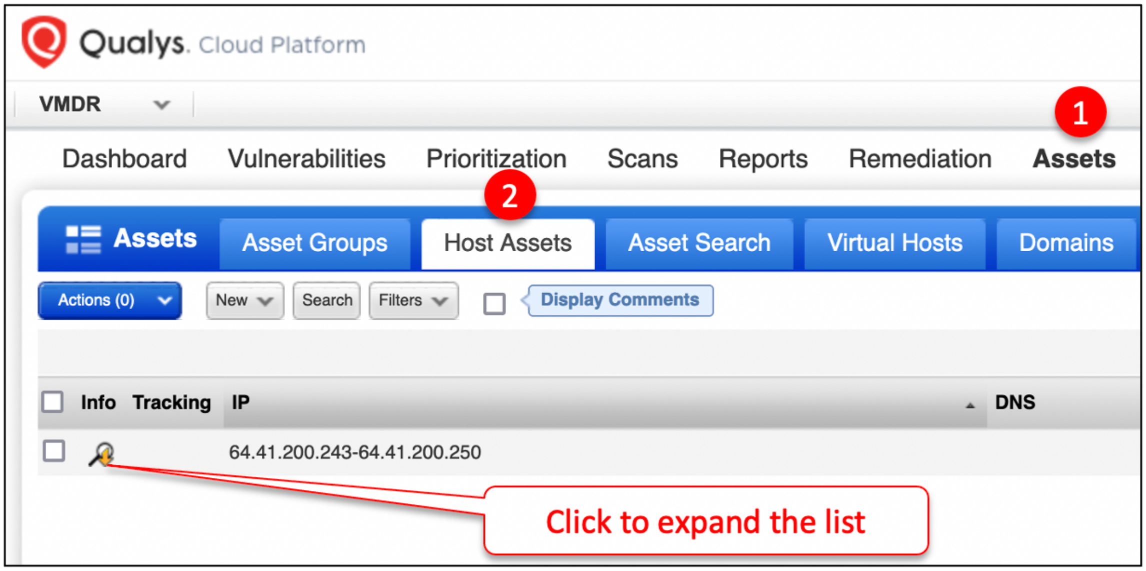
- Last VM scan is greater than 7 days
- Any of the following Information Gathered are present
  -IG 105015 Windows Authentication Failed
  -IG 105053 Unix Authentication Failed

You can also use asset tag rules based on asset search queries, vulnerability QIDs or groovy scriplets to automatically identify and tag assets for purging.

Once stale records are identified and validated, you can purge via the UI or API.

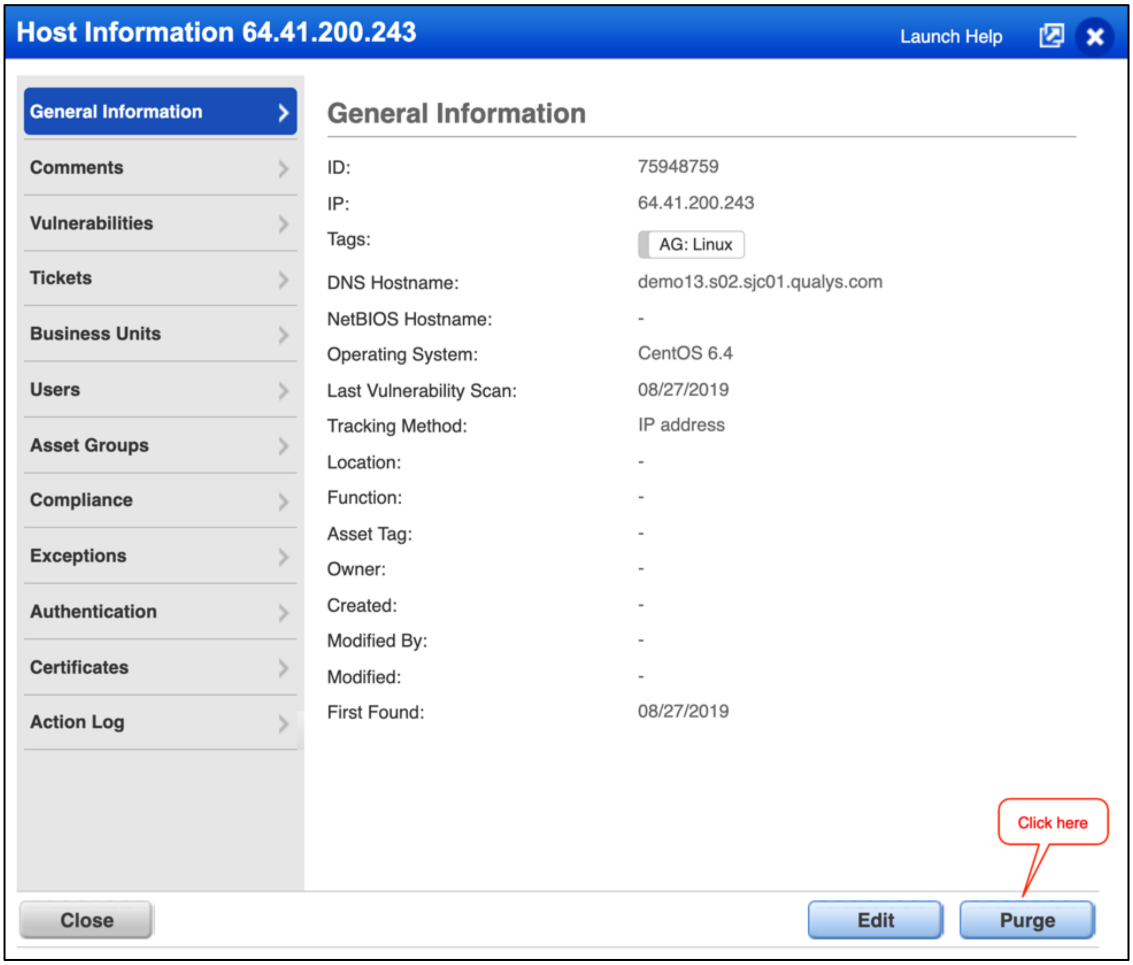
Purge an IP

Purging an IP will remove the scan data without removing the IP from your account.



□	Info	Tracking	IP	DNS
□			64.41.200.243-64.41.200.250	

Click to expand the list

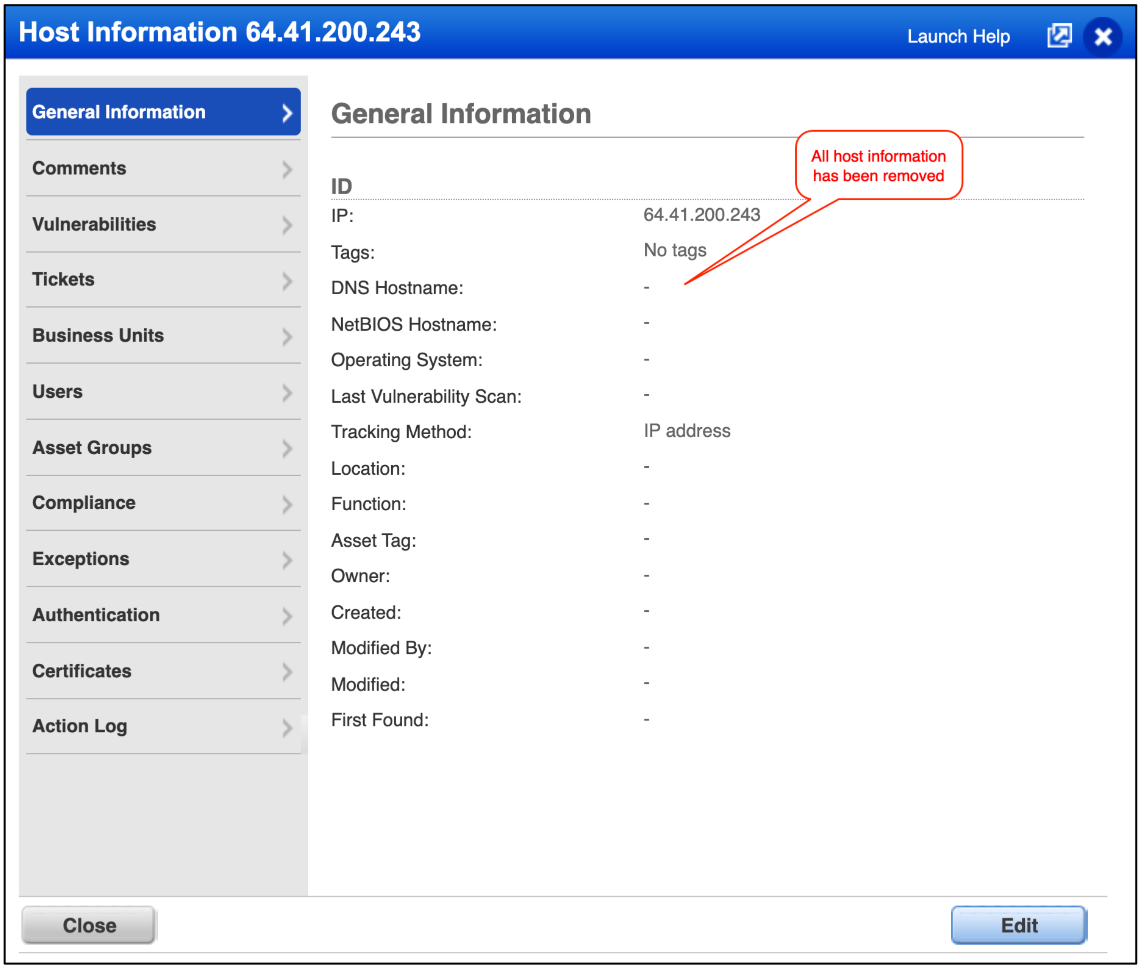


Host Information 64.41.200.243

General Information

ID:	75948759
IP:	64.41.200.243
Tags:	AG: Linux
DNS Hostname:	demo13.s02.sjc01.qualys.com
NetBIOS Hostname:	-
Operating System:	CentOS 6.4
Last Vulnerability Scan:	08/27/2019
Tracking Method:	IP address
Location:	-
Function:	-
Asset Tag:	-
Owner:	-
Created:	-
Modified By:	-
Modified:	-
First Found:	08/27/2019

Purging can take a while. View the host information again to confirm host vulnerability information is removed. After the purging operation completes, all host information such as hostname, operating system, last scan date, tags, comments, vulnerabilities, and tickets will be removed.



General Information

ID

IP:	64.41.200.243
Tags:	No tags
DNS Hostname:	-
NetBIOS Hostname:	-
Operating System:	-
Last Vulnerability Scan:	-
Tracking Method:	IP address
Location:	-
Function:	-
Asset Tag:	-
Owner:	-
Created:	-
Modified By:	-
Modified:	-
First Found:	-

All host information has been removed

Navigate to the following URL to view the lab tutorial for this topic:

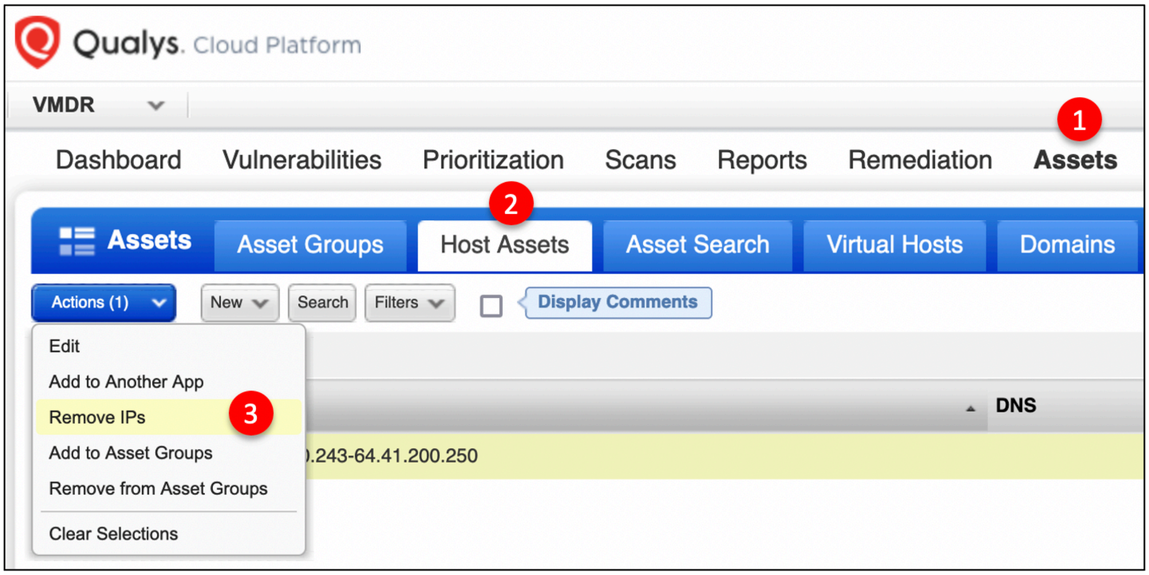
PLAY

Lab: Purging Hosts

https://ior.ad/7AIv

Removing an IP

When an IP is removed, associated host-based scan data is permanently removed, and the IP is no longer available for scanning and reporting.



Note that once you purge or remove an asset, all host scan data (findings) for the asset is removed from your Qualys account, and this action is irreversible. So, consider exporting host scan data for the concerned asset before purging or removing the asset. We recommend using Qualys APIs for exporting this data as APIs are better suited for bulk data export operations.

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Removing Hosts

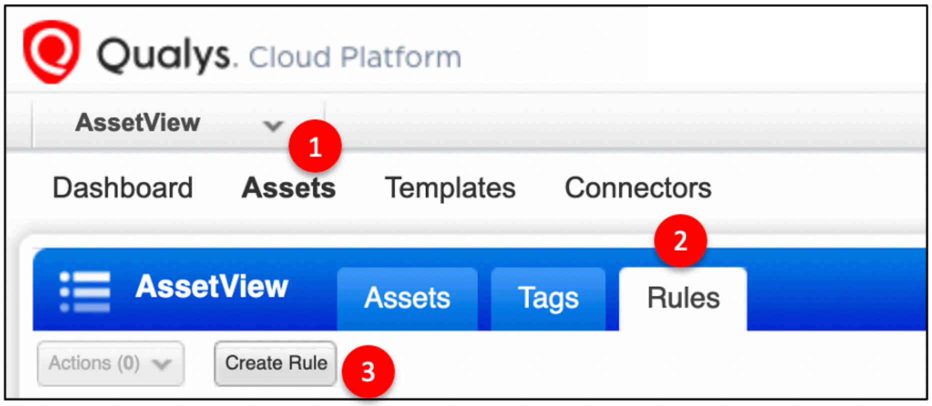
https://ior.ad/7AIw

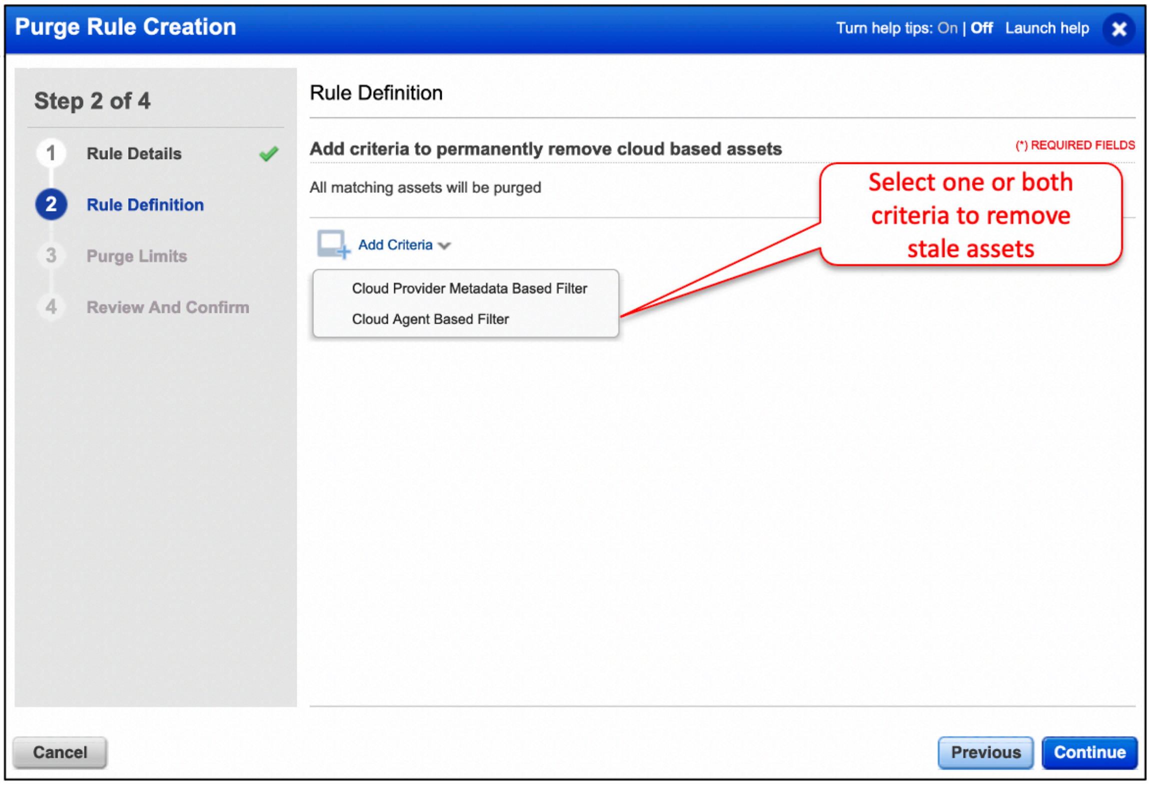
Rule-based Purge

You can define purge rules to automatically purge assets and cloud agents based on the terminated/deallocated state of the cloud instance or time since last activity or vulnerability scan. Your purge rules will run daily. When you purge an asset this way, you remove the asset and the data associated with it.

This feature must be enabled for your subscription. Please reach out to Qualys Support or your Technical Account Manager to have this capability enabled.

When enabled for your subscription, you can purge these types of assets:
- EC2 assets discovered by AWS connectors
- Assets discovered by Azure connectors and cloud agents
- Google Cloud Platform (GCP) assets discovered by cloud agents
- Cloud agent assets




Purge Rule Creation
Turn help tips: On | Off Launch help
Step 2 of 4
1 Rule Details
2 Rule Definition
3 Purge Limits
4 Review And Confirm
Rule Definition
Add criteria to permanently remove cloud based assets
(*) REQUIRED FIELDS
All matching assets will be purged
Add Criteria
Cloud Provider Metadata Based Filter
Cloud Agent Based Filter
Select one or both criteria to remove stale assets
Cancel
Previous
Continue

Note: There is no lab tutorial for rule-based purging.

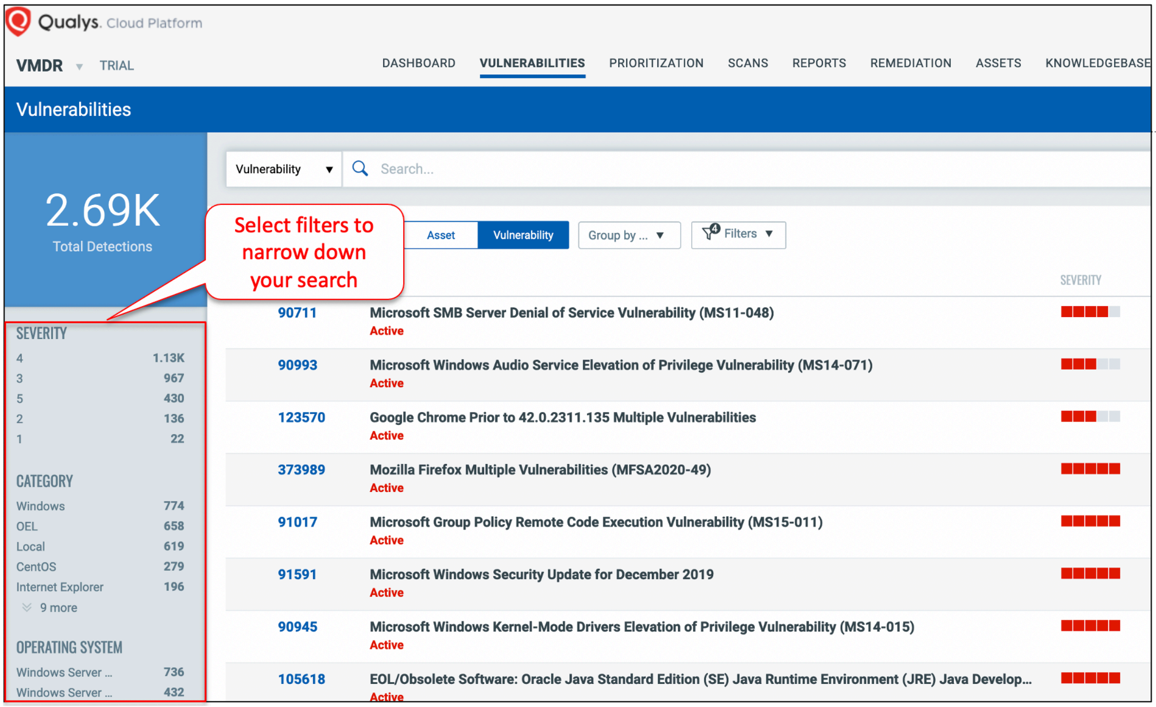
LAB 4: VM/VMDR Dashboard (Time: 20 mins)

VMDR Dashboard gives you a complete and continuously updated view of all your VM assets – on-prem, endpoints and in the cloud, in one place within the VM module. Vulnerability and security results are correlated from VM scans and cloud agents

Search Filters

VMDR search capabilities give you the ability to quickly find all about your assets and vulnerabilities in one place.

You can use the available metadata filters to refine your search results.



2.69K
Total Detections

Select filters to narrow down your search

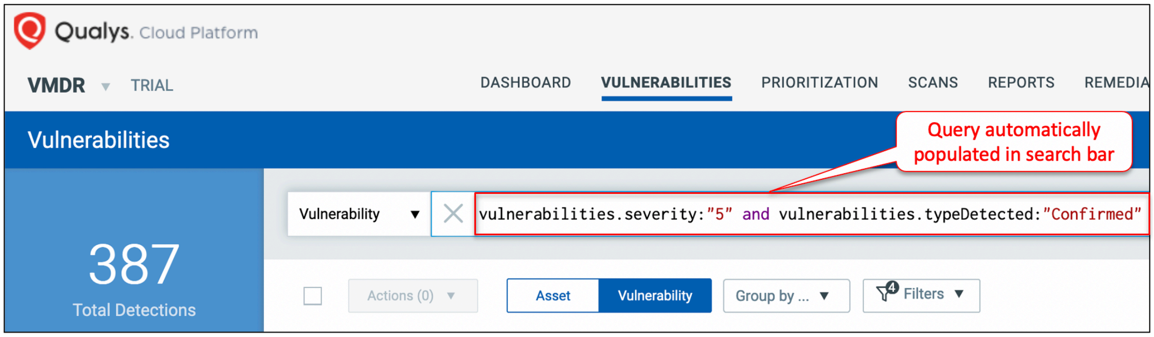
SEVERITY	
4	1.13K
3	967
5	430
2	136
1	22

CATEGORY	
Windows	774
OEL	658
Local	619
CentOS	279
Internet Explorer	196
9 more	

OPERATING SYSTEM	
Windows Server ...	736
Windows Server ...	432

		SEVERITY
90711	Microsoft SMB Server Denial of Service Vulnerability (MS11-048) Active	■■■■□
90993	Microsoft Windows Audio Service Elevation of Privilege Vulnerability (MS14-071) Active	■■■□□
123570	Google Chrome Prior to 42.0.2311.135 Multiple Vulnerabilities Active	■■■□□
373989	Mozilla Firefox Multiple Vulnerabilities (MFSA2020-49) Active	■■■■■
91017	Microsoft Group Policy Remote Code Execution Vulnerability (MS15-011) Active	■■■■■
91591	Microsoft Windows Security Update for December 2019 Active	■■■■■
90945	Microsoft Windows Kernel-Mode Drivers Elevation of Privilege Vulnerability (MS14-015) Active	■■■■■
105618	EOL/Obsolete Software: Oracle Java Standard Edition (SE) Java Runtime Environment (JRE) Java Develop... Active	■■■■■

As you select the filters on the left-hand side, a query will be automatically formed in the search bar.



```
vulnerabilities.severity:"5" and vulnerabilities.typeDetected:"Confirmed"
```

Query automatically populated in search bar

Navigate to the following URL to view the lab tutorial for this topic:

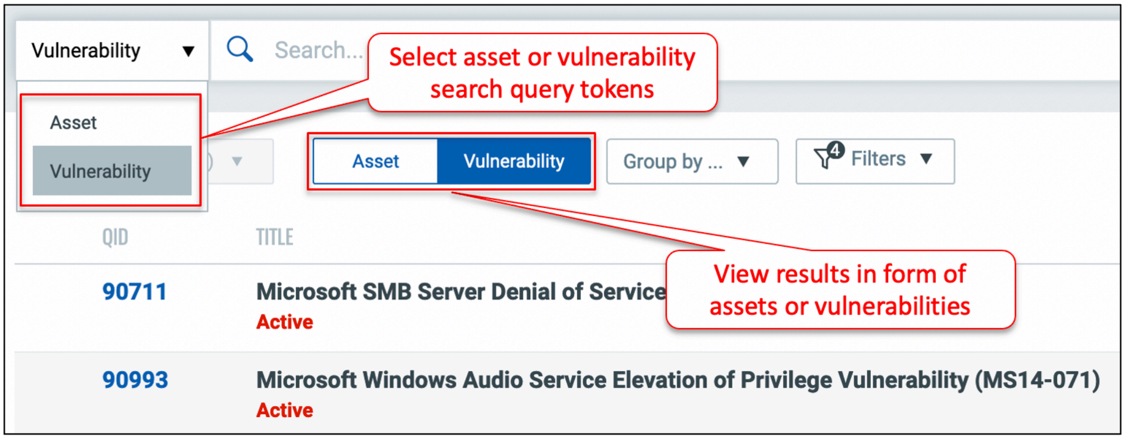
Lab: Faceted Search

https://ior.ad/7AIA

Search Queries

The VM/VMDR dashboard allows you form queries based on assets or vulnerabilities. Note: Before performing the queries, it is a good idea to look at the query formatting best practices - Dashboard Toolbox - Improving Dashboard Performance through Query Formatting and Filters

Choose Vulnerability to display vulnerability data (like we did here), or Asset for asset data. You can easily browse the data list and explore details.



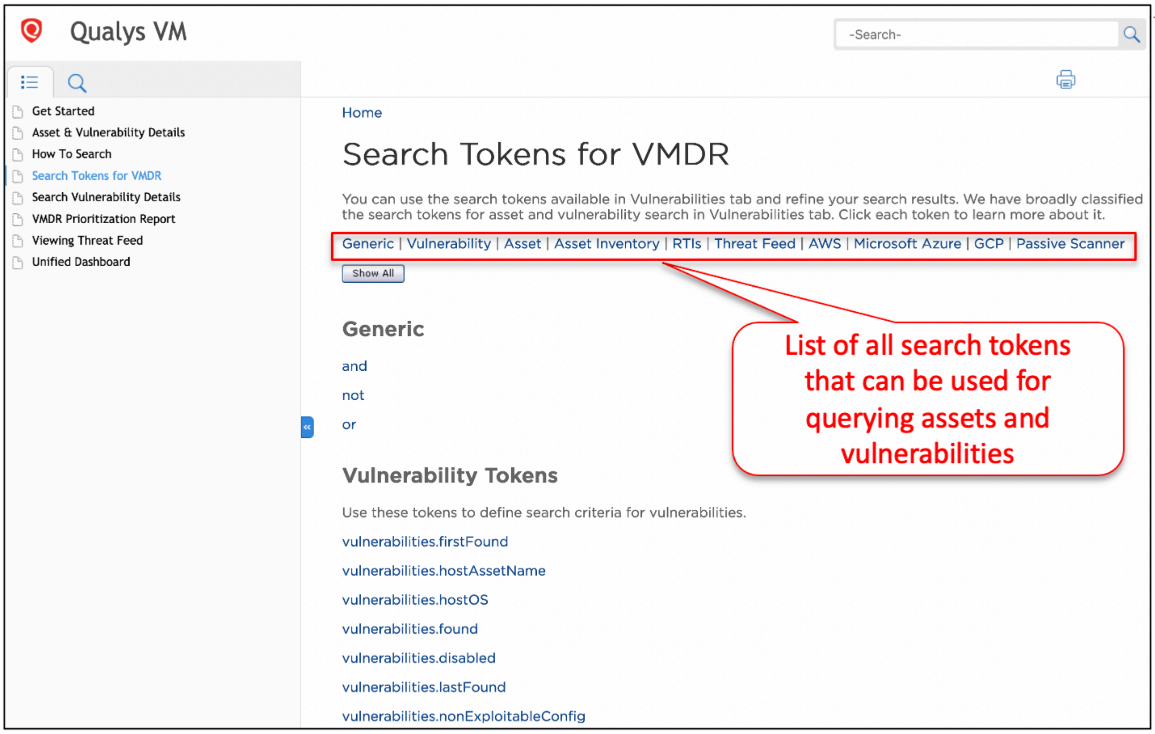
Select asset or vulnerability search query tokens

View results in form of assets or vulnerabilities

QID	TITLE
90711	Microsoft SMB Server Denial of Service Active
90993	Microsoft Windows Audio Service Elevation of Privilege Vulnerability (MS14-071) Active

You can use multiple query tokens to define criteria for searching assets and asset properties, vulnerabilities, Real Time Threat Indicators (RTIs), Threat Feeds, AWS, Azure and Google cloud assets on the asset list and others.

Use Qualys Online Help to find more information on available tokens.



Search Tokens for VMDR

You can use the search tokens available in Vulnerabilities tab and refine your search results. We have broadly classified the search tokens for asset and vulnerability search in Vulnerabilities tab. Click each token to learn more about it.

Generic | Vulnerability | Asset | Asset Inventory | RTIs | Threat Feed | AWS | Microsoft Azure | GCP | Passive Scanner

List of all search tokens that can be used for querying assets and vulnerabilities

Generic

and

not

or

Vulnerability Tokens

Use these tokens to define search criteria for vulnerabilities.

vulnerabilities.firstFound

vulnerabilities.hostAssetName

vulnerabilities.hostOS

vulnerabilities.found

vulnerabilities.disabled

vulnerabilities.lastFound

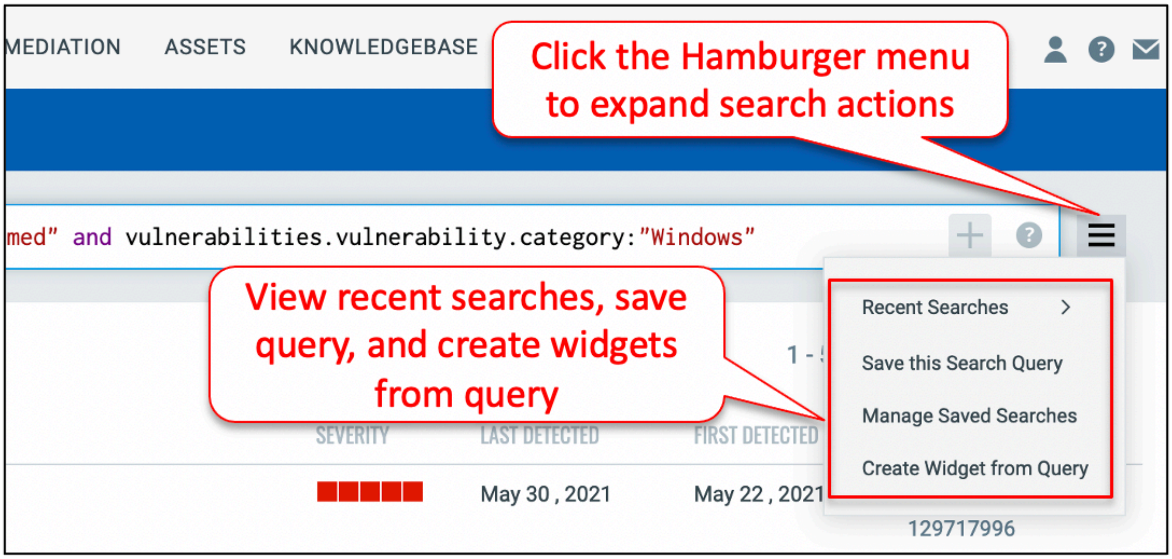
vulnerabilities.nonExploitableConfig

Note that some tokens will be limited based on your organization's subscription. Please consult your Qualys Technical Account Manager to know more about your subscription type.

Search Actions

You could always save a search query and make it readily available for use. You can view the frequently-used QQL queries, save, and manage them with ease. You can also create widgets from the frequently-used queries for easy reference in future.

Recent Searches: We save your last five search query history. You can quickly pick the search query from the list and use it without the need to build it from scratch.

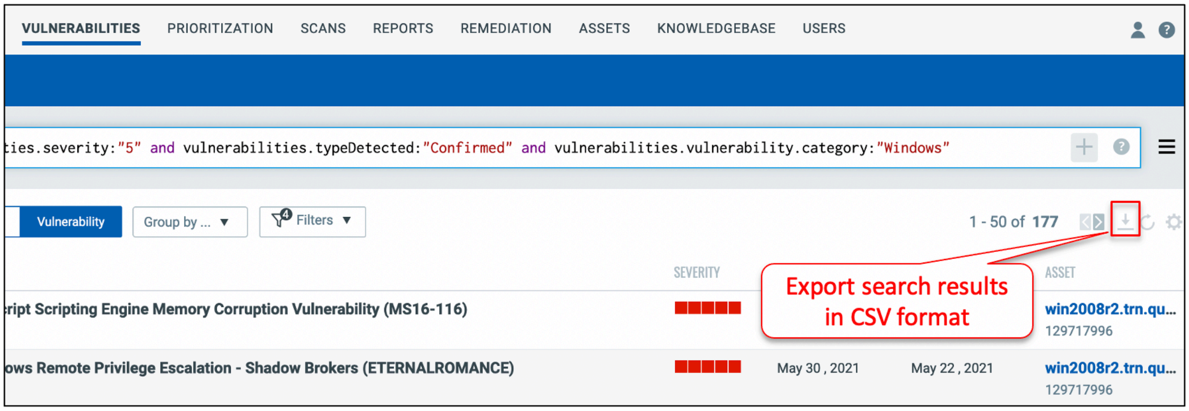


Click the Hamburger menu to expand search actions

View recent searches, save query, and create widgets from query

`med" and vulnerabilities.vulnerability.category:"Windows"`

You can also export the search results to your local system and share them with other users. You can export results in CSV format. It just takes a minute to export search results.



Export search results in CSV format

`ies.severity:"5" and vulnerabilities.typeDetected:"Confirmed" and vulnerabilities.vulnerability.category:"Windows"`

Note that the download is limited to 10,000 vulnerability records.

Navigate to the following URL to view the lab tutorial for this topic:

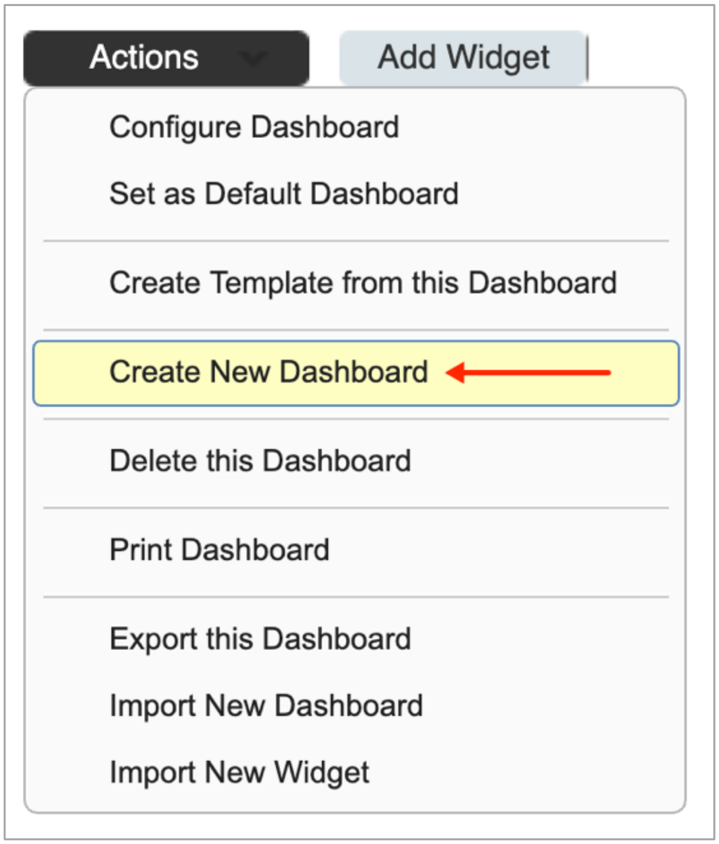
PLAY **Lab**: Search Queries

https://ior.ad/7AIy

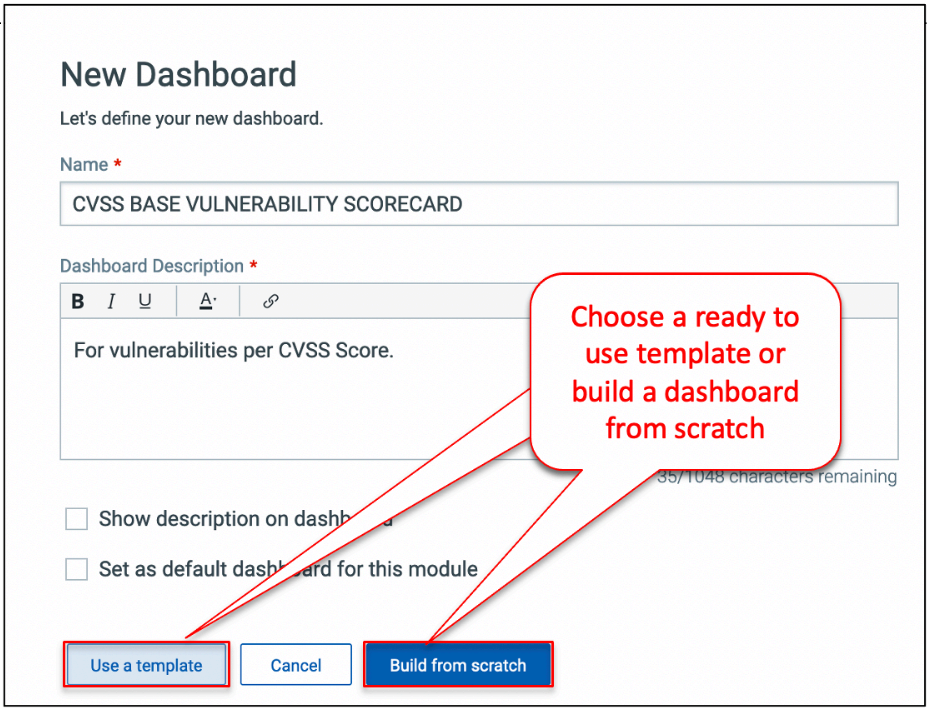
Dashboards and Widgets

Qualys provides ready to use templates for dashboards that you can quickly add to your list of dashboards and start monitoring your assets and vulnerabilities.

Qualys publishes new templates regularly and these are automatically added to the template library in your Qualys account.



When you select the “Use a template” option to create a dashboard, you’ll see a list of pre-configured dashboards to select from.



New Dashboard

Let's define your new dashboard.

Name *

CVSS BASE VULNERABILITY SCORECARD

Dashboard Description *

For vulnerabilities per CVSS Score.

35/1048 characters remaining

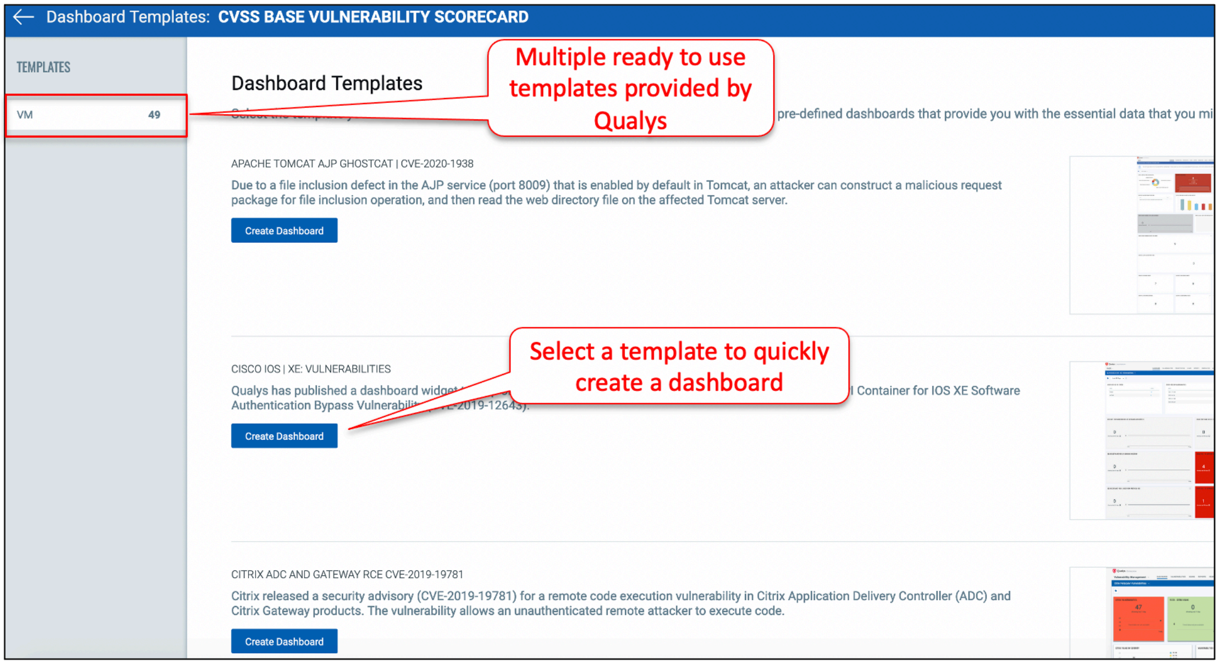
□ Show description on dashb

□ Set as default dash ard for this module

Choose a ready to use template or build a dashboard from scratch

Amongst the templates, choose the one that suits your need of data population for your assets and create a dashboard. Your dashboard will be ready to use.

You can add more widgets to your dashboard, edit existing widgets, change the layout of widgets and perform many more things in your dashboard.



Dashboard Templates: **CVSS BASE VULNERABILITY SCORECARD**

Dashboard Templates

pre-defined dashboards that provide you with the essential data that you mi

APACHE TOMCAT AJP GHOSTCAT | CVE-2020-1938

Due to a file inclusion defect in the AJP service (port 8009) that is enabled by default in Tomcat, an attacker can construct a malicious request package for file inclusion operation, and then read the web directory file on the affected Tomcat server.

CISCO IOS | XE: VULNERABILITIES

Qualys has published a dashboard widget l Container for IOS XE Software Authentication Bypass Vulnerabili 2019-12643).

CITRIX ADC AND GATEWAY RCE CVE-2019-19781

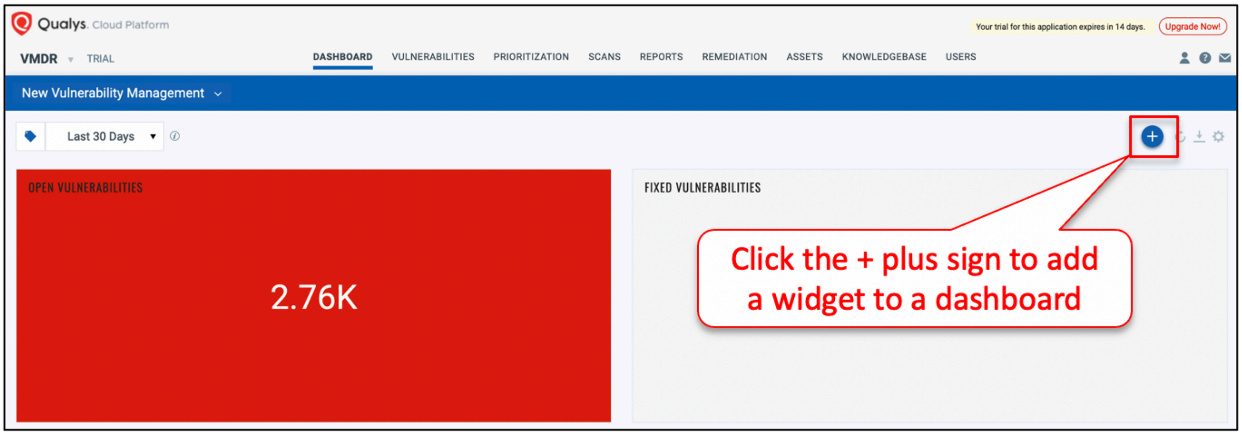
Citrix released a security advisory (CVE-2019-19781) for a remote code execution vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway products. The vulnerability allows an unauthenticated remote attacker to execute code.

Multiple ready to use templates provided by Qualys

Select a template to quickly create a dashboard

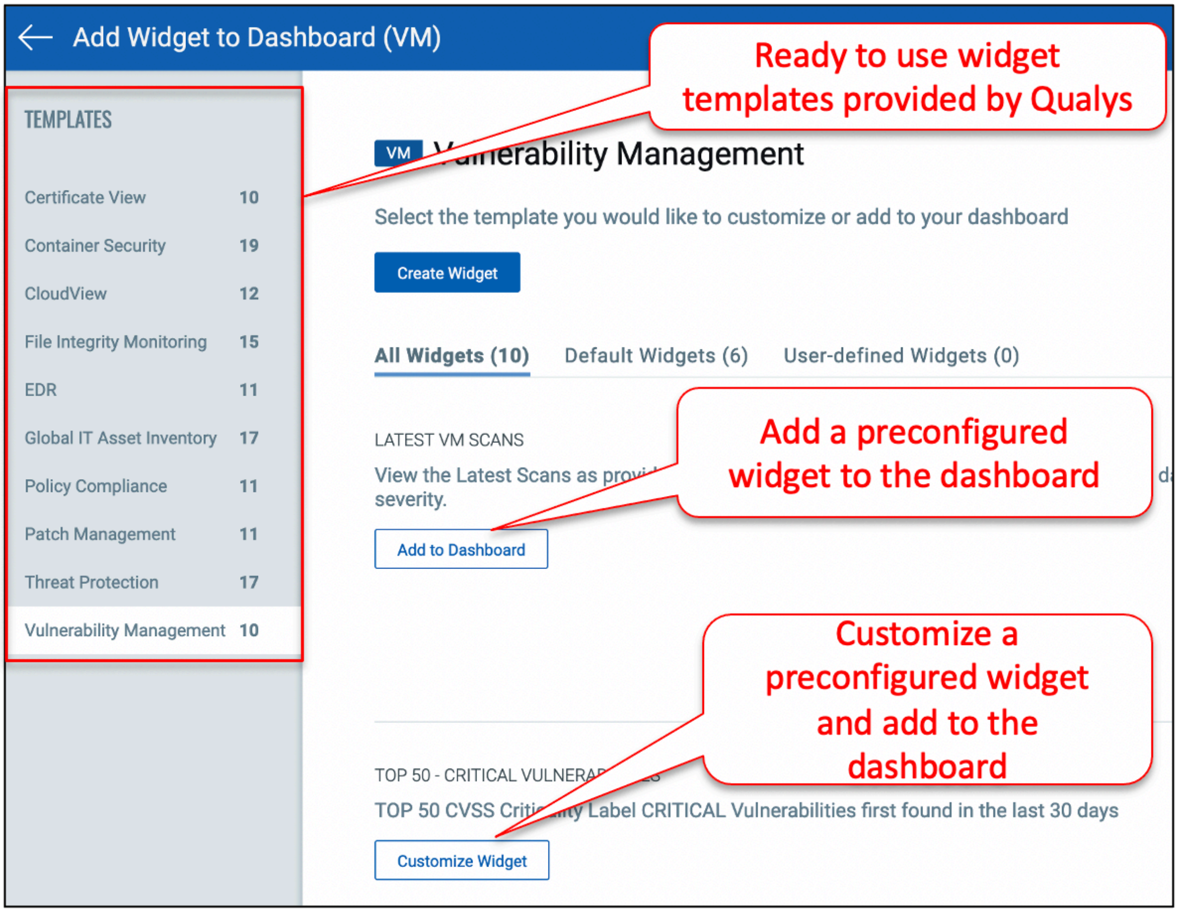
Add a Preconfigured Widget and Customize it

You can add pre-configured readymade widgets into your dashboards.



Click the + plus sign to add a widget to a dashboard

You can add the widget template to the dashboard or further customize the template to suit your need.



TEMPLATES	
Certificate View	10
Container Security	19
CloudView	12
File Integrity Monitoring	15
EDR	11
Global IT Asset Inventory	17
Policy Compliance	11
Patch Management	11
Threat Protection	17
Vulnerability Management	10

Select the template you would like to customize or add to your dashboard

View the Latest Scans as provi severity.

TOP 50 CVSS Criti ity Label CRITICAL Vulnerabilities first found in the last 30 days

Ready to use widget templates provided by Qualys

Add a preconfigured widget to the dashboard

Customize a preconfigured widget and add to the dashboard

Navigate to the following URL to view the lab tutorial for this topic:

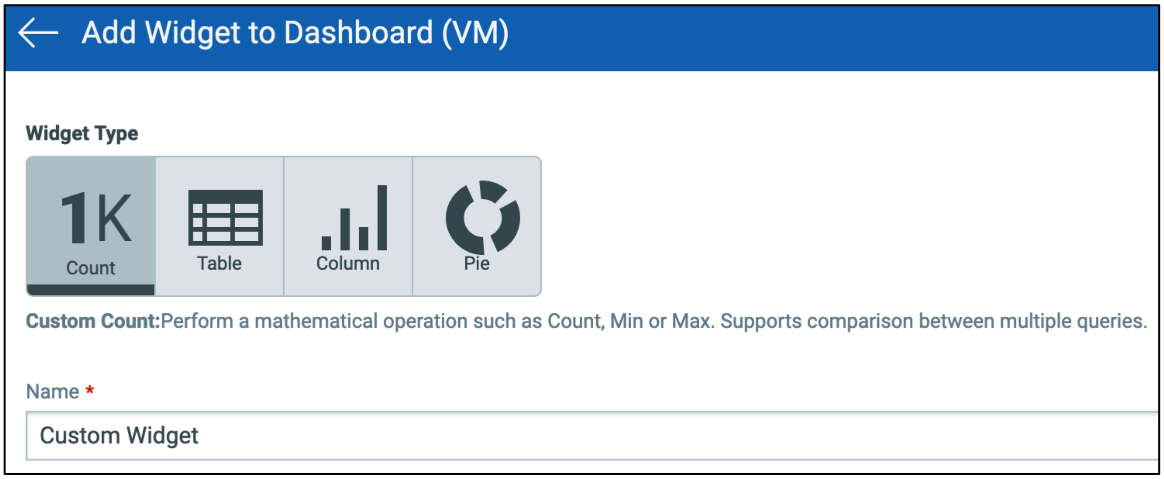
PLAY **Lab**: Create Dashboards and Widgets Using Templates
https://ior.ad/7AIB

Create widgets from scratch

You could also create your own widget from scratch. Just about any query that you build can be used to create a dashboard widget that displays useful graphics and/or statistics. You can add as many widgets as you like to customize your vulnerability posture view.

The widget builder displays all the applications/modules in your subscription. Select the module for which you want to pick the data to be populated in the widget.

We provide four types of widgets:
- Count
- Table
- Column
- Pie



Custom Count: Perform a mathematical operation such as Count, Min or Max. Supports comparison between multiple queries.

Name *

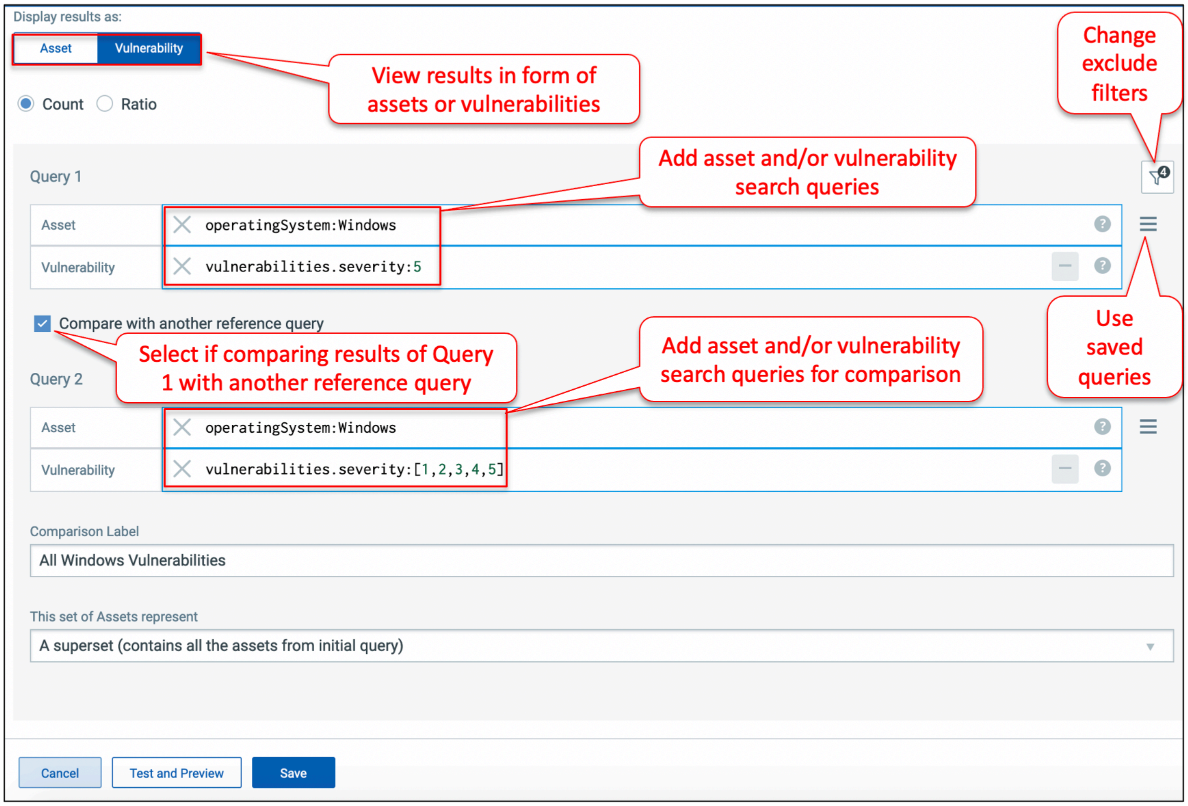
Custom Widget

You can fetch data and display the count of mathematical operation in a count widget. You could also compare numbers with multiple queries. For example, if you want to view the count of malicious files or count of missing patches or assets, where patch installation is pending.

Use table type of widget when you have multiple data points to be grouped by certain parameters. For example, if you want to view the top 10 operating systems that are infected or the missing patches information for each vendor type you could use table widget.

Use column or bar graph type of widget when you want to multiple search criteria to be monitored. For example, if you want to view vulnerabilities that belong to certain criteria on assets that meet different criteria.

Use pie chart type of widget when you want to illustrate multiple data points through a numerical proportion in a circular statistical graphic. For example, if you want to show the breakdown of vulnerabilities by status (New, Active, Fixed & Reopened) through a numerical proportion.



● Count ○ Ratio

Query 1

Asset: operatingSystem:Windows

Vulnerability: vulnerabilities.severity:5

☑ Compare with another reference query

Query 2

Asset: operatingSystem:Windows

Vulnerability: vulnerabilities.severity:[1,2,3,4,5]

Comparison Label: All Windows Vulnerabilities

This set of Assets represent: A superset (contains all the assets from initial query)

View results in form of assets or vulnerabilities

Add asset and/or vulnerability search queries

Change exclude filters

Use saved queries

Select if comparing results of Query 1 with another reference query

Add asset and/or vulnerability search queries for comparison

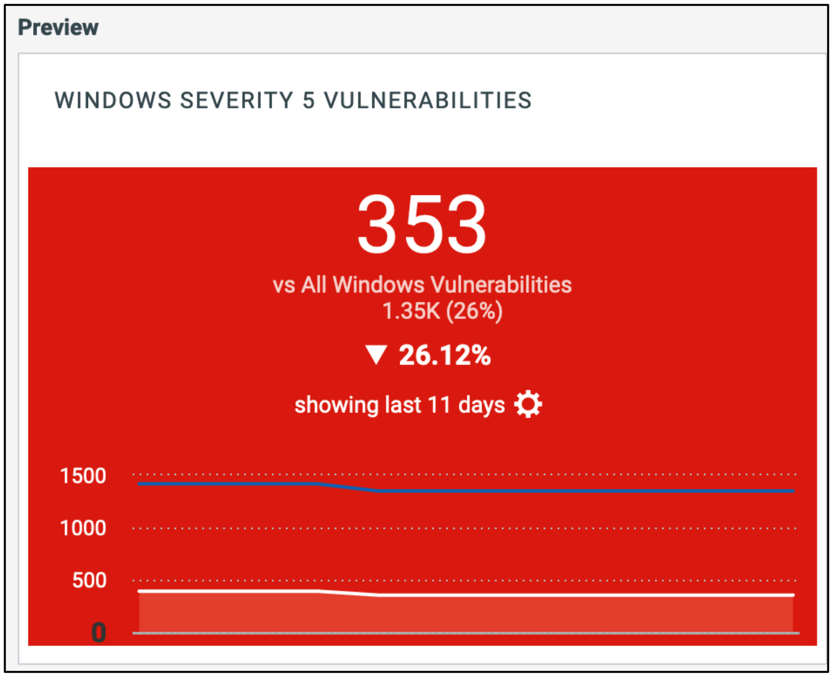
Depending on the widget type you choose, populate the information required for the widget.

Type in your search query for the data to be populated in the widget.

Select check box to enable comparison data between two data points. For the second data point to be populated, provide the search query for comparison, a label for the count, and choose if the second data point is superset, subset or a distinct set of the first query you provided.

If you do not provide another reference query to compare against, the service automatically compares your matching asset count against the total count of all assets.

Click Test and Preview to test how the search query works and get a preview of your widget.



Preview

WINDOWS SEVERITY 5 VULNERABILITIES

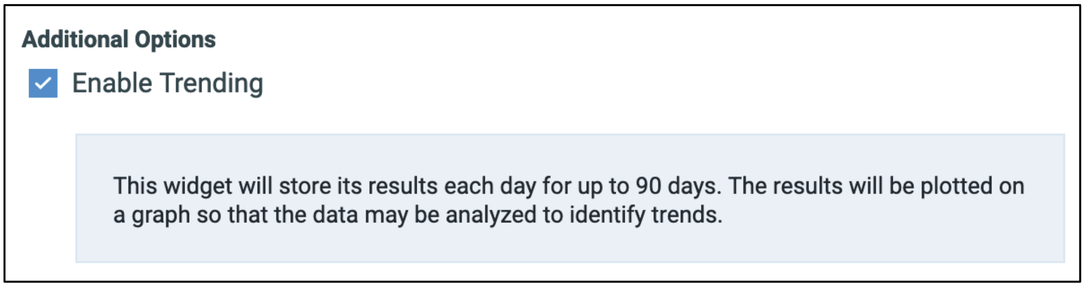
353

vs All Windows Vulnerabilities
1.35K (26%)

▼ 26.12%

showing last 11 days

You can also configure dashboard count widgets to display trend data. Enable the Collect trend data option in the dynamic widget wizard. Once enabled, the widget trend data is collected daily and stored for up to 90 days. This is used to plot a line graph in the count widget.

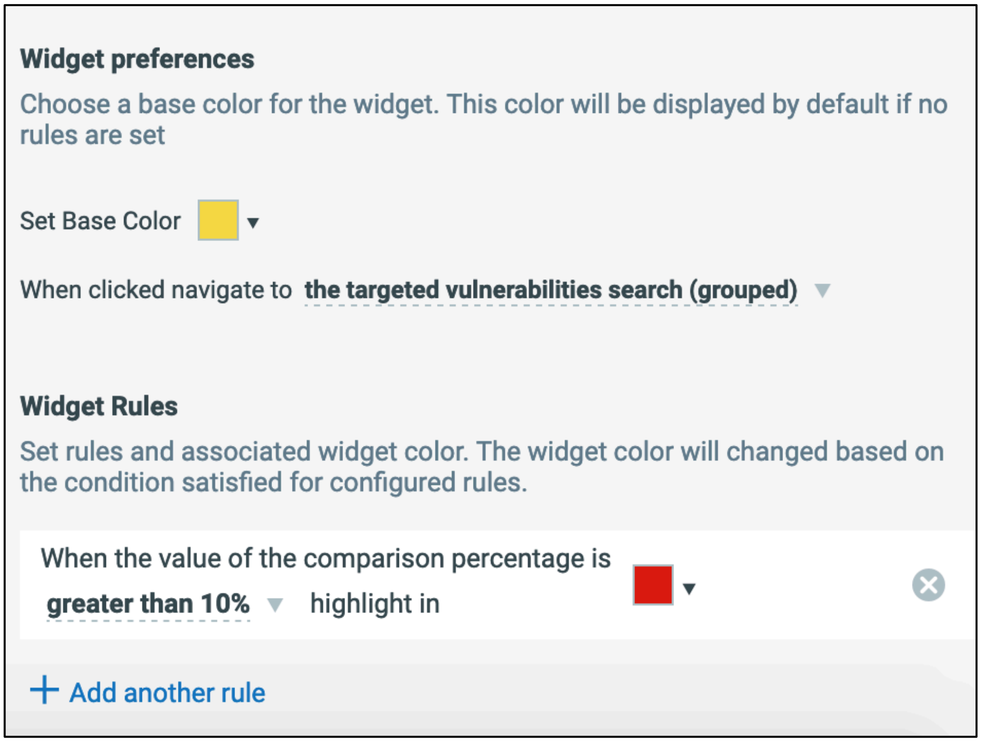


Additional Options

☑ Enable Trending

This widget will store its results each day for up to 90 days. The results will be plotted on a graph so that the data may be analyzed to identify trends.

You can also configure the widget preferences such as background color, navigation for data points.



Widget preferences

Choose a base color for the widget. This color will be displayed by default if no rules are set

Set Base Color 🟨 ▾

When clicked navigate to **the targeted vulnerabilities search (grouped)** ▾

Widget Rules

Set rules and associated widget color. The widget color will changed based on the condition satisfied for configured rules.

When the value of the comparison percentage is **greater than 10%** ▾ highlight in 🟥 ▾ ⊗

Set Base Color: Define the background color to be used for the widget for quick identification.

When clicked navigate to: Configure the navigation path or the data list screen to be displayed when

Widget Rules: You could define criteria in form of rules for the widget. For example, if you want the widget to alert you by change in color when it meets a certain threshold, you could add a rule for the same. You can also define multiple criteria for the widget.

If there are multiple rules defined for the widget and if the widget matches multiple rules, the last rule that meets the criteria is implemented.

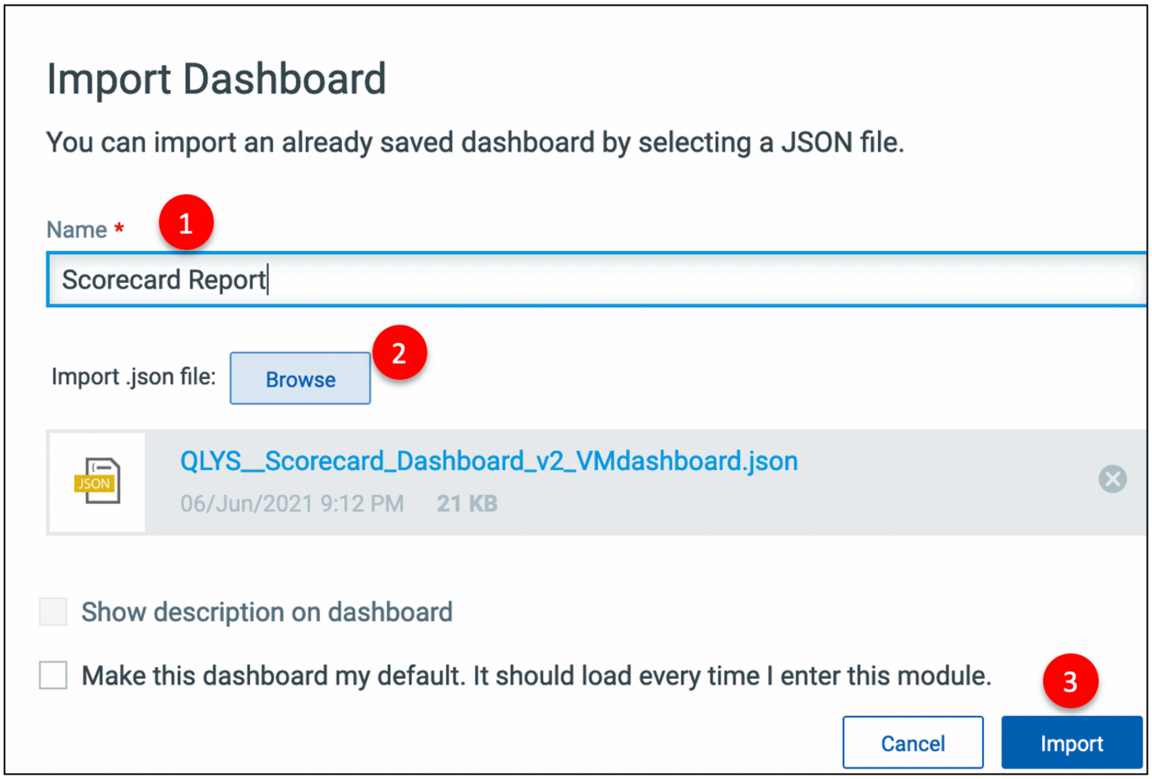
Navigate to the following URL to view the lab tutorial for this topic:

PLAY **Lab**: Create Custom Widgets

https://ior.ad/7Bz0

Import a Dashboard

You can export and import dashboard and widget configurations to a file in a JSON format allowing you to share them between accounts or within the Qualys community. You'll find a lot of useful, ready-to-use dashboards available on the Qualys community.



Import Dashboard

You can import an already saved dashboard by selecting a JSON file.

Name * 1

Scorecard Report

Import .json file: Browse 2

QLYS__Scorecard_Dashboard_v2_VMdashboard.json
06/Jun/2021 9:12 PM 21 KB

□ Show description on dashboard

□ Make this dashboard my default. It should load every time I enter this module. 3

Click Browse and browse to the dashboard file (JSON format) to be imported and click Import.

The dashboard file downloaded from the Qualys Community or the exported file (JSON format) cannot be edited as it is encrypted for security purposes. You can directly import the file (but cannot edit) to view the dashboard.

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Import a Dashboard

https://ior.ad/7AIx

LAB 5: Threat Protection (Time: 5 mins)

A vulnerability becomes a greater risk when it has an associated threat. Threat Protection helps you visualize and assess your actual security threats in one place.

Threat Protection has an up-to-date feed of the latest threats and how they could potentially affect your environment. It gives you the ability to prioritize the real threats to your organization. Threat Protection provides context to your data by correlating your vulnerability data (obtained via scans/cloud agent) to actual threats.

Threat Protection is a part of VMDR and provides Real-Time Threat Indicators to the Prioritization Report, that will help you identify the potential impact of discovered vulnerabilities, as well as vulnerabilities that have known or existing threats.

Understand use of RTIs in VMDR Prioritization Report (The tutorial link given below is from the VMDR training course)

PLAY

VMDR Prioritization

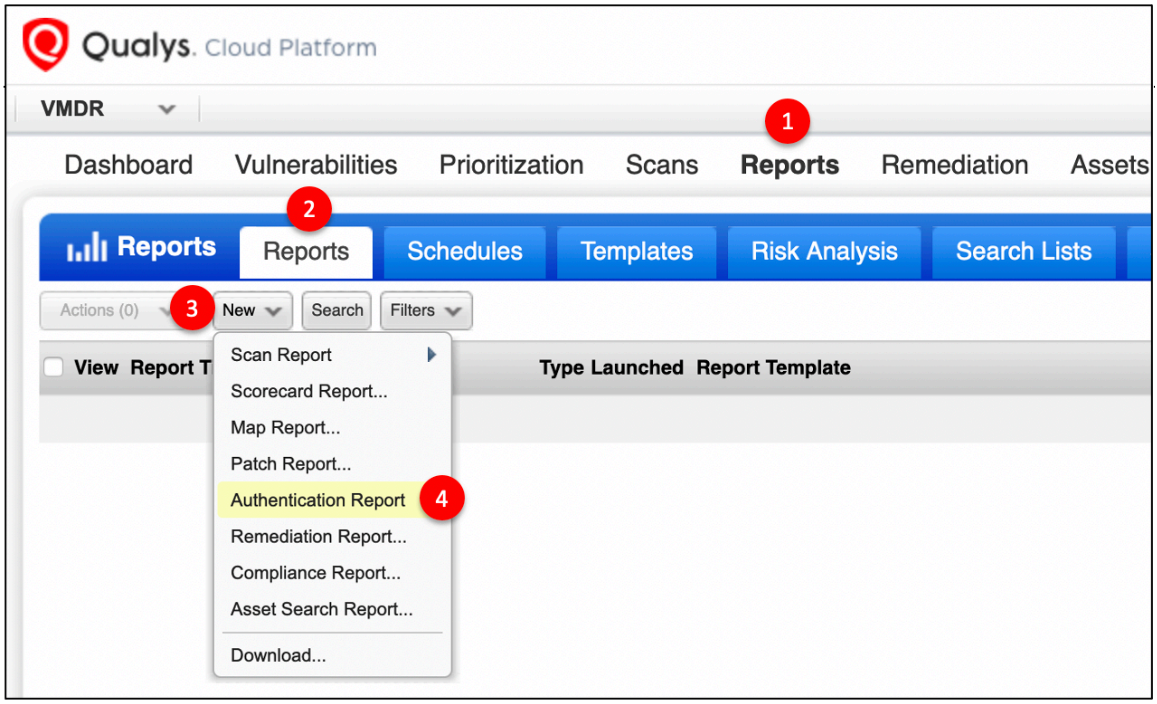
http://ior.ad/7dEE

LAB 6: Authentication Report (Time: 5 mins)

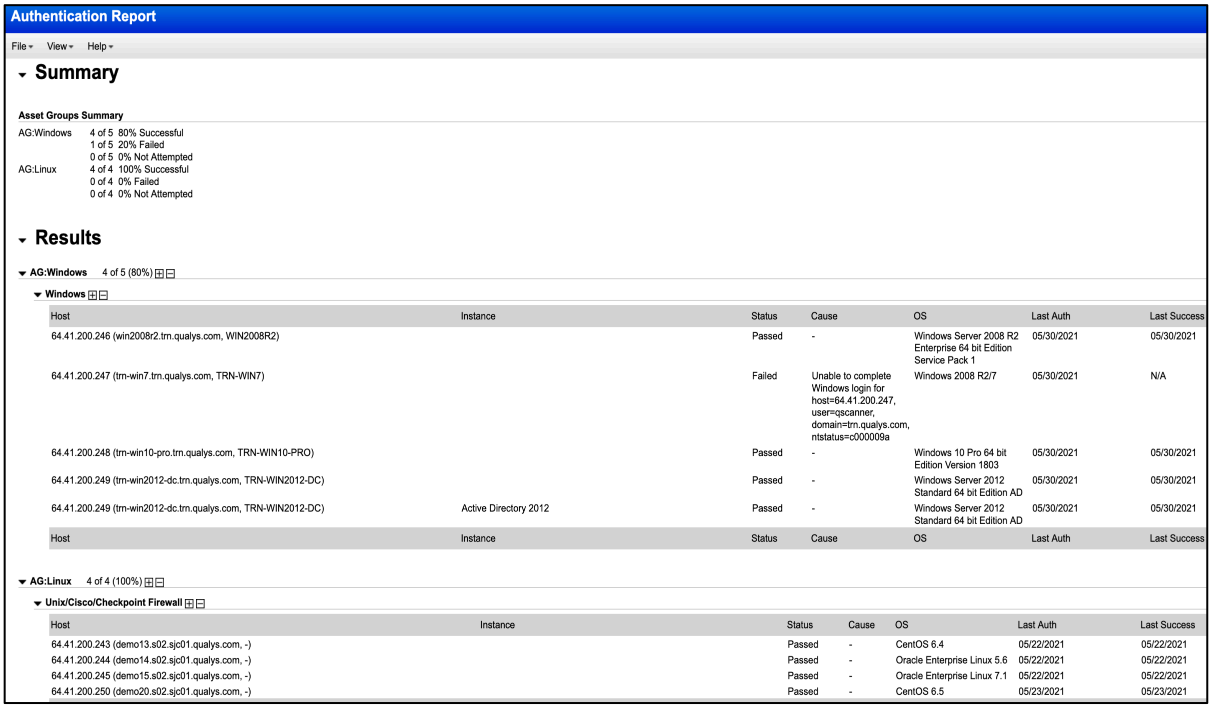
You can create an Authentication Report to identify authentication PASS/FAIL results and troubleshoot authentication issues.

***IMPORTANT**: You must have at least one "Finished" authenticated scan to create an Authentication Report.*

Best Practice - Schedule this report to run frequently to help you manage and address authentication issues.



For each IP, business unit, asset group or asset tag included in the report, you'll see the total number of hosts at each authentication status level. For example, if your report shows "4 of 6 66% Successful" for a particular asset group, then 6 hosts in the asset group were successfully scanned. Out of the 6 hosts scanned, the scanning engine was able to authenticate to 4 hosts. This means that the scanning engine authenticated to 66% of the scanned hosts for the group.



Summary

Asset Groups Summary

AG:Windows	4 of 5	80% Successful
	1 of 5	20% Failed
	0 of 5	0% Not Attempted
AG:Linux	4 of 4	100% Successful
	0 of 4	0% Failed
	0 of 4	0% Not Attempted

Results

AG:Windows 4 of 5 (80%) ⊞ ⊟

Windows ⊞ ⊟

Host	Instance	Status	Cause	OS	Last Auth	Last Success
64.41.200.246 (win2008r2.trn.qualys.com, WIN2008R2)		Passed	-	Windows Server 2008 R2 Enterprise 64 bit Edition Service Pack 1	05/30/2021	05/30/2021
64.41.200.247 (trn-win7.trn.qualys.com, TRN-WIN7)		Failed	Unable to complete Windows login for host=64.41.200.247, user=qscanner, domain=trn.qualys.com, ntstatus=c000009a	Windows 2008 R2/7	05/30/2021	N/A
64.41.200.248 (trn-win10-pro.trn.qualys.com, TRN-WIN10-PRO)		Passed	-	Windows 10 Pro 64 bit Edition Version 1803	05/30/2021	05/30/2021
64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)		Passed	-	Windows Server 2012 Standard 64 bit Edition AD	05/30/2021	05/30/2021
64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)	Active Directory 2012	Passed	-	Windows Server 2012 Standard 64 bit Edition AD	05/30/2021	05/30/2021
Host	Instance	Status	Cause	OS	Last Auth	Last Success

AG:Linux 4 of 4 (100%) ⊞ ⊟

Unix/Cisco/Checkpoint Firewall ⊞ ⊟

Host	Instance	Status	Cause	OS	Last Auth	Last Success
64.41.200.243 (demo13.s02.sjc01.qualys.com, -)		Passed	-	CentOS 6.4	05/22/2021	05/22/2021
64.41.200.244 (demo14.s02.sjc01.qualys.com, -)		Passed	-	Oracle Enterprise Linux 5.6	05/22/2021	05/22/2021
64.41.200.245 (demo15.s02.sjc01.qualys.com, -)		Passed	-	Oracle Enterprise Linux 7.1	05/22/2021	05/22/2021
64.41.200.250 (demo20.s02.sjc01.qualys.com, -)		Passed	-	CentOS 6.5	05/23/2021	05/23/2021

Authentication Status:

Passed – Authentication was successful.

Failed – Authentication failed. Review the “Cause” column.

Passed* - Authentication was successful but with insufficient privileges (applies to the Qualys Policy Compliance application only)

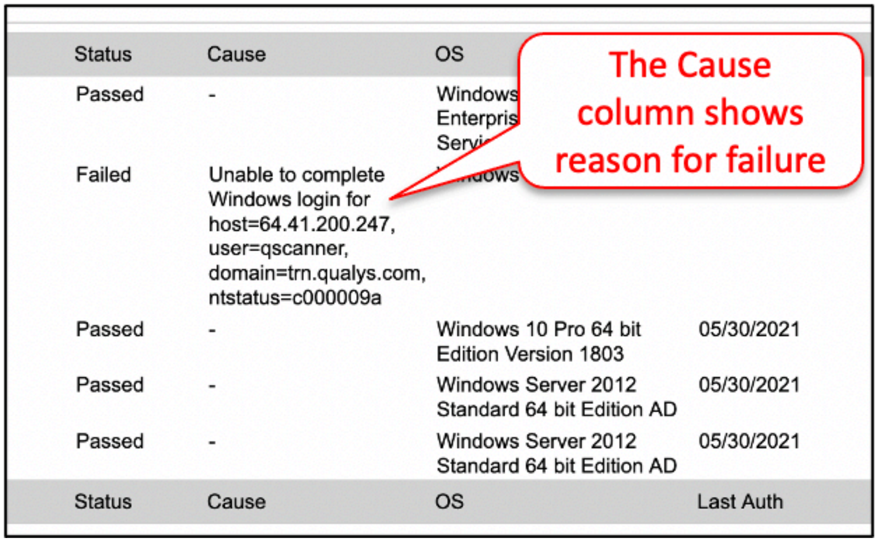
Not Attempted – The scanner appliance was unable to locate an authentication record for the asset or authentication was not turned on in the Option Profile.

You'll see Last Auth and Last Success dates in your report when "Additional Host Info" was selected at run time.

Last Auth - The last time each host was scanned using authentication - this is when the status was last updated to Passed or Failed.
Last Success - The last time authentication was successful for each host. N/A indicates that the host has been scanned with authentication enabled but it has not been successful.

Troubleshoot a Failed Authentication Attempt

Check out the Cause column to get the login ID used during the authentication attempt. Review your authentication record for the host/type and the account privileges to troubleshoot the issue.



The Cause column shows reason for failure

Status	Cause	OS	
Passed	-	Windows Enterpris Servi	
Failed	Unable to complete Windows login for host=64.41.200.247, user=qscanner, domain=trn.qualys.com, ntstatus=c000009a	dows	
Passed	-	Windows 10 Pro 64 bit Edition Version 1803	05/30/2021
Passed	-	Windows Server 2012 Standard 64 bit Edition AD	05/30/2021
Passed	-	Windows Server 2012 Standard 64 bit Edition AD	05/30/2021
Status	Cause	OS	Last Auth

Authentication Dashboards

You can also use dashboards to track authentication status. Dashboards enable you to be more pro-active in your authentication management of Qualys Scans. Pre-built VM/VMDR dashboard JSON files for Windows Authentication Management are available on the following link:
https://qualys-secure.force.com/discussions/s/article/000006159

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Authentication Report

https://ior.ad/7B2Z

The hosts used in the Qualys Training Lab are impacted by multiple factors, and results may vary from day-to-day. You will find that one Windows host with IP address 64.41.200.47 (hostname: TRN-WIN7) reports a failed authentication status in the Authentication Report. And so vulnerability results displayed in various lab simulations in this training only include status of remotely discoverable vulnerability QIDs for this host.

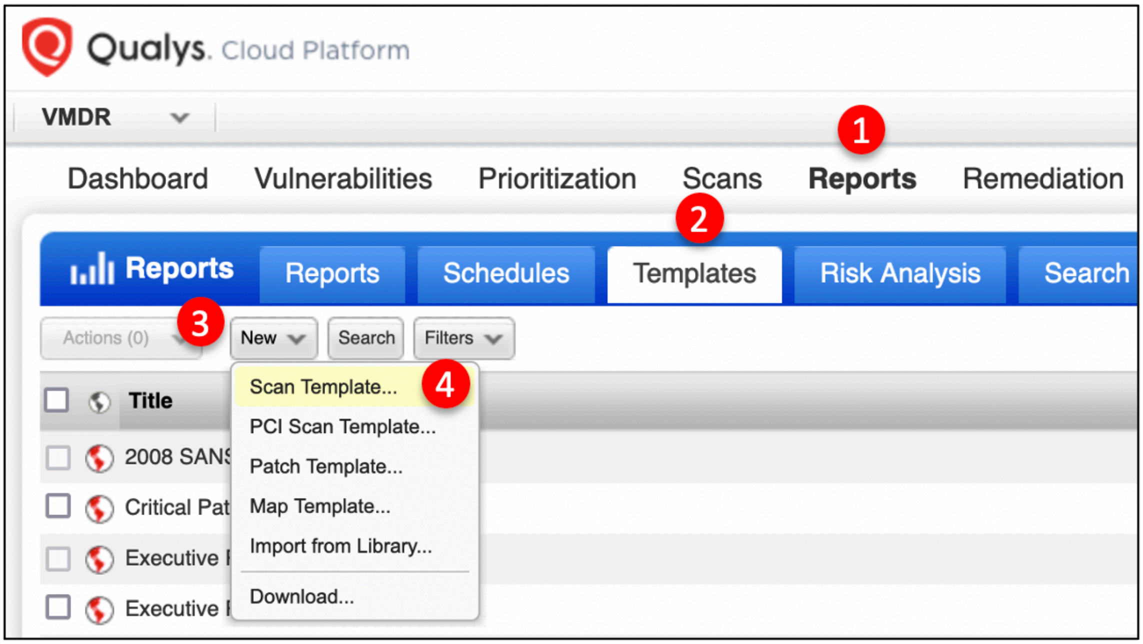
LAB 7: Host Based and Scan Based Findings (Time: 15 mins)

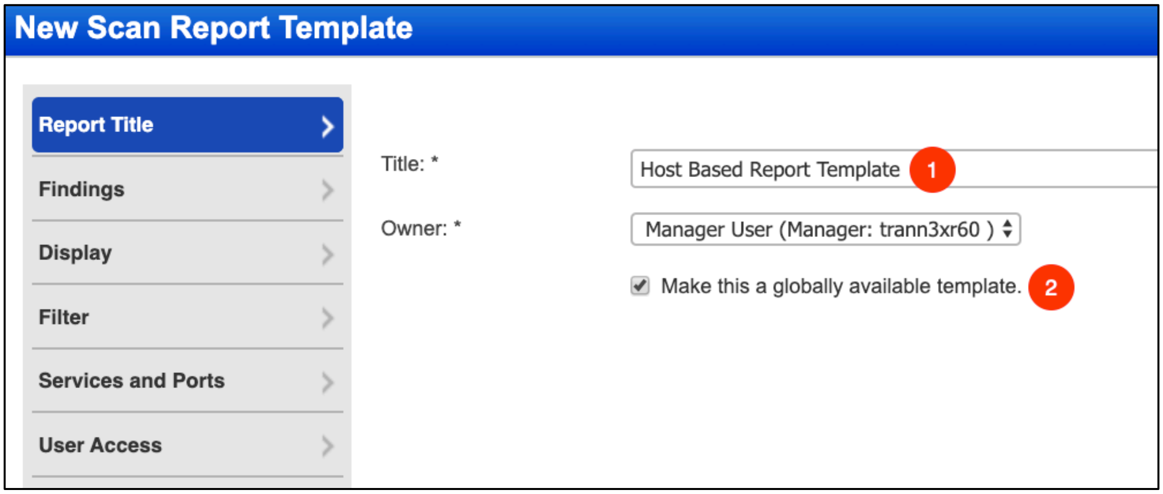
The Scan Report Template is the most popular way to filter and prioritize vulnerability findings. In the forthcoming labs, you will investigate the different functionality of the Scan Report Template, starting first with the "Findings" options.

***IMPORTANT**: A host scan or assessment must be performed prior to building a vulnerability report. The scan or assessment data can be collected using either a Qualys Scanner Appliance or Qualys Cloud Agent.*

Host Based Findings Report Template

Host Based Findings gives you the most comprehensive and up to date picture of your vulnerability status. It encompasses the latest vulnerability data from all of your scans. This lab will begin with an example of a "Host Based Findings" report. Customized report template examples are provided for both Host Based and Scan Based reports.



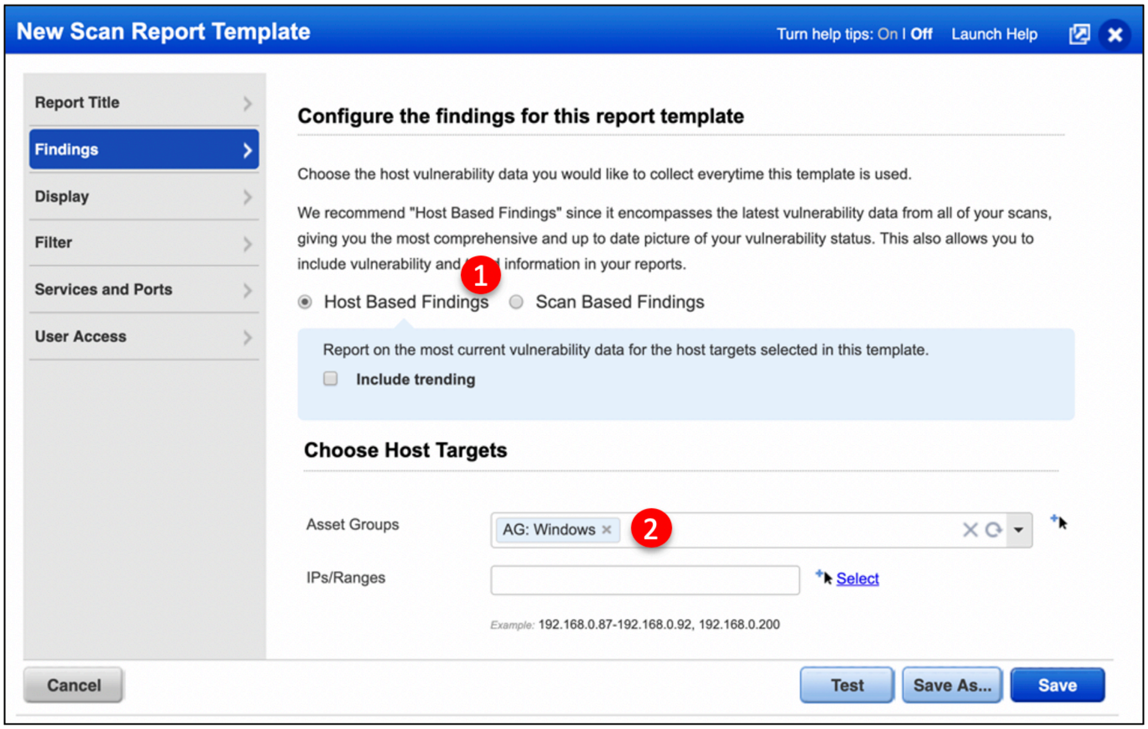


Title: * Host Based Report Template

Owner: * Manager User (Manager: trann3xr60)

☑ Make this a globally available template.

Templates that are "globally available" can be used by other Qualys users to create their own reports (using this custom template).



Configure the findings for this report template

Choose the host vulnerability data you would like to collect everytime this template is used.

We recommend "Host Based Findings" since it encompasses the latest vulnerability data from all of your scans, giving you the most comprehensive and up to date picture of your vulnerability status. This also allows you to include vulnerability and l information in your reports.

● Host Based Findings ○ Scan Based Findings

Report on the most current vulnerability data for the host targets selected in this template.

□ **Include trending**

Choose Host Targets

Asset Groups: AG: Windows ×

IPs/Ranges:

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

The "Findings" section of a Scan Report Template provides separate options for Host Based Findings and Scan Based Findings.

Although "trending" is a common option for reports that use Host Based Findings, it will not be useful until you have performed vulnerability scans and assessments for several days (to establish some type of vulnerability history).

IMPORTANT: The target you select here, will become the "default" for all reports created with this template. Avoid using the built-in Asset Group called "All" as a report template target (especially for accounts that have a significant number of host assets). To avoid creating reports that require significant processing time, Qualys recommends using more specific or focused targets.

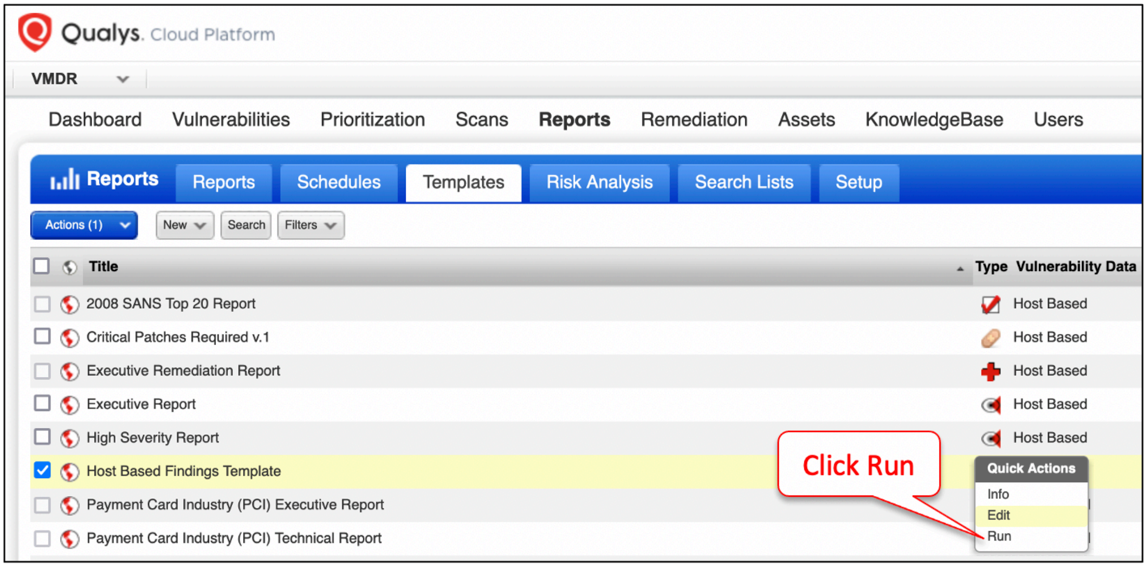
Navigate to the following URL to view the lab tutorial for this topic:

Lab: Host Based template

https://ior.ad/7Bb1

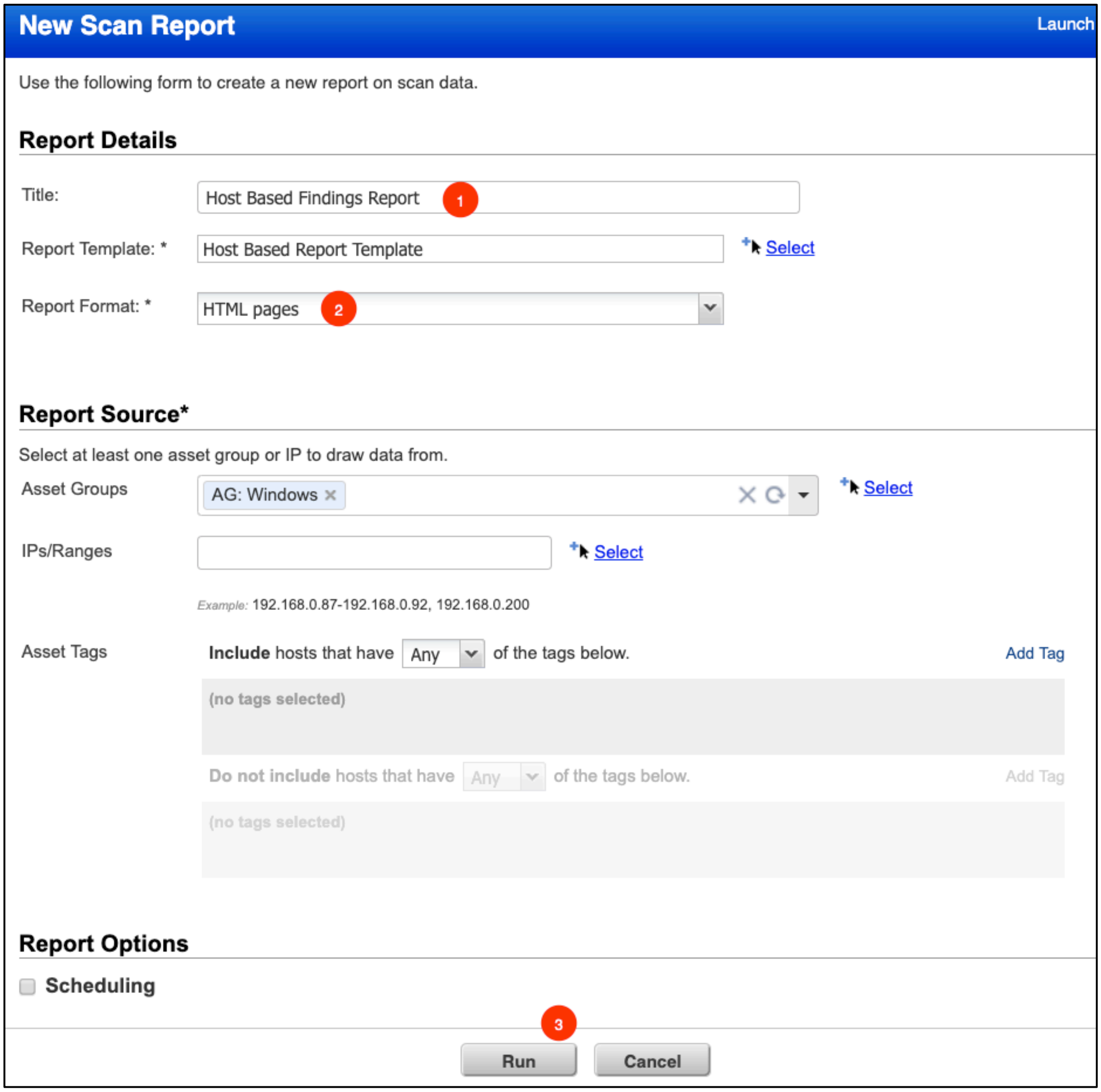
Create Host Based Findings Report

Use your customized host-based findings report template to generate (run) a report.



☐	Title	Type	Vulnerability Data
☐	2008 SANS Top 20 Report		Host Based
☐	Critical Patches Required v.1		Host Based
☐	Executive Remediation Report		Host Based
☐	Executive Report		Host Based
☐	High Severity Report		Host Based
☑	Host Based Findings Template		
☐	Payment Card Industry (PCI) Executive Report		
☐	Payment Card Industry (PCI) Technical Report		

Click Run



New Scan Report Launch

Use the following form to create a new report on scan data.

Report Details

Title: Host Based Findings Report (1)

Report Template: * Host Based Report Template Select

Report Format: * HTML pages (2)

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups: AG: Windows ✕ Select

IPs/Ranges: Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags: **Include** hosts that have Any of the tags below. Add Tag

(no tags selected)

Do not include hosts that have Any of the tags below. Add Tag

(no tags selected)

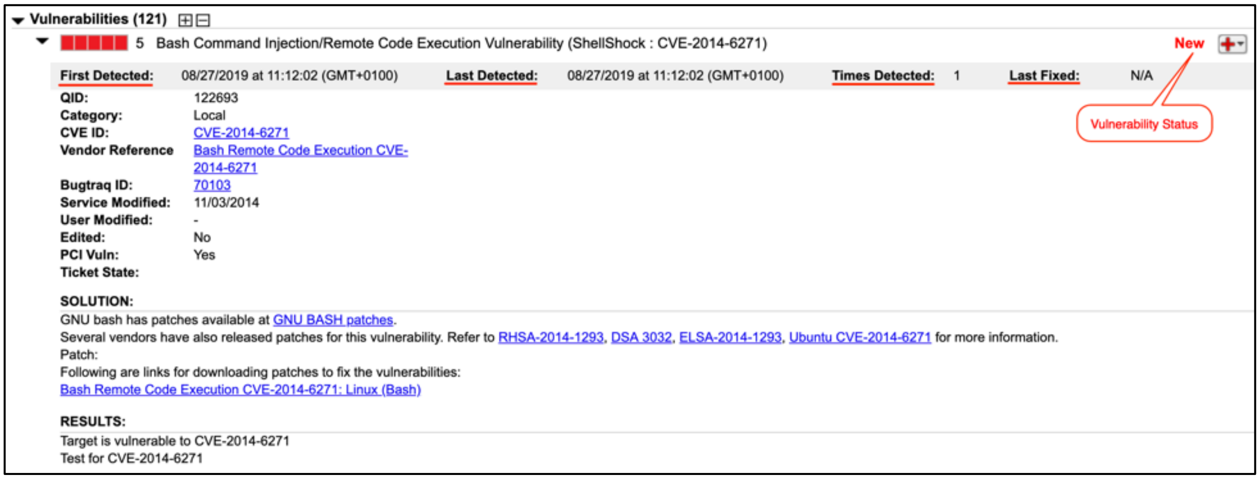
Report Options

□ **Scheduling**

(3)

While the GUI allows you to change the Report Source, reports that are generated through Qualys' Application Program Interface (API), often do not have the option to select a different target. For this reason, Qualys recommends avoiding the use of the Asset Group called "All" when creating a report template.

When your report is displayed, you can scroll down to the "Detailed Results" section and expand any vulnerability.



Vulnerabilities (121)

5 Bash Command Injection/Remote Code Execution Vulnerability (ShellShock : CVE-2014-6271) New

First Detected: 08/27/2019 at 11:12:02 (GMT+0100) **Last Detected:** 08/27/2019 at 11:12:02 (GMT+0100) **Times Detected:** 1 **Last Fixed:** N/A

QID:	122693
Category:	Local
CVE ID:	CVE-2014-6271
Vendor Reference	Bash Remote Code Execution CVE-2014-6271
Bugtraq ID:	70103
Service Modified:	11/03/2014
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	

SOLUTION:

GNU bash has patches available at GNU BASH patches.
Several vendors have also released patches for this vulnerability. Refer to RHSA-2014-1293, DSA 3032, ELSA-2014-1293, Ubuntu CVE-2014-6271 for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Bash Remote Code Execution CVE-2014-6271: Linux (Bash)

RESULTS:

Target is vulnerable to CVE-2014-6271
Test for CVE-2014-6271

If your assets have been scanned only once, the vulnerabilities will have a "New" status. If they have been scanned more than once, they will have an "Active" status.

Also, notice the "First Detected," "Last Detected," "Times Detected," and "Last Fixed" dates that track the evolution of any finding.

This information can help you determine the time it has taken to fix a vulnerability; from the time it was first detected.

Also, if there is a wide gap between "Last Detected" date and the report date, this may be an indicator that you need to perform another scan.

Navigate to the following URL to view the lab tutorial for this topic:

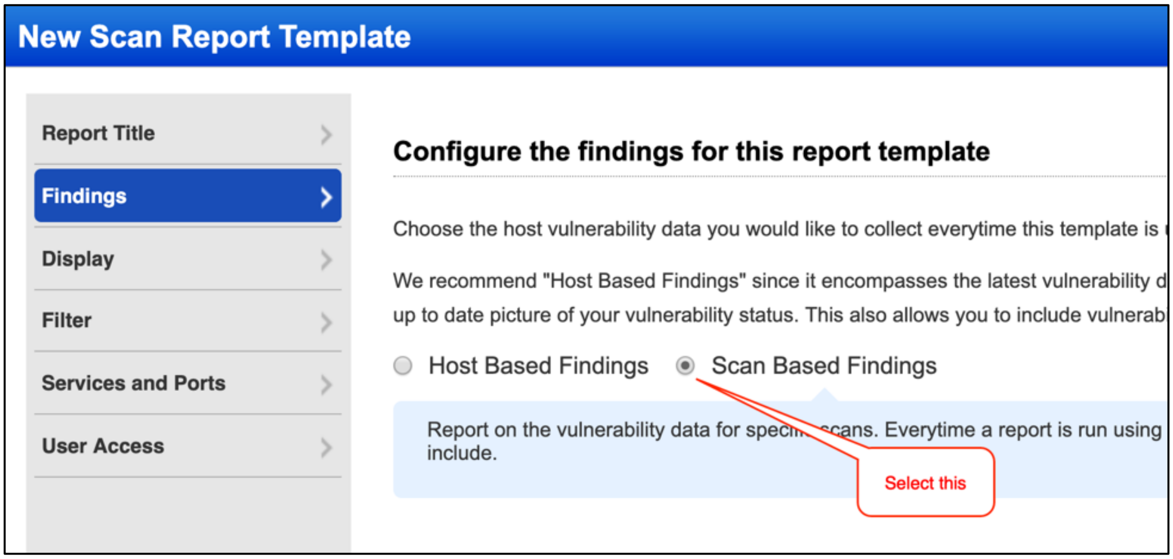
PLAY

Lab: Host Based Report

https://ior.ad/7Bb2

Scan Based Findings Report Template

In this section, you will build a template that uses Scan Based Findings, to create a report that targets one host in one scan. This technique will save you report processing time by focusing on the host of interest while eliminating those that are irrelevant.



Configure the findings for this report template

Choose the host vulnerability data you would like to collect everytime this template is

We recommend "Host Based Findings" since it encompasses the latest vulnerability d up to date picture of your vulnerability status. This also allows you to include vulnerab

○ Host Based Findings ● Scan Based Findings

Report on the vulnerability data for specific scans. Everytime a report is run using include.

Notice that you no longer have the ability to choose Asset Groups, Tags, or individual IP addresses after selecting this option. Scan Based findings allow you select from saved scan results. When running a report with this template, you will be prompted to select the scan results. Because Scan Based Findings do not reflect any "historical" or "future" vulnerability findings, they are said to represent a "snapshot" in time; each scan represents one snapshot.

Navigate to the following URL to view the lab tutorial for this topic:

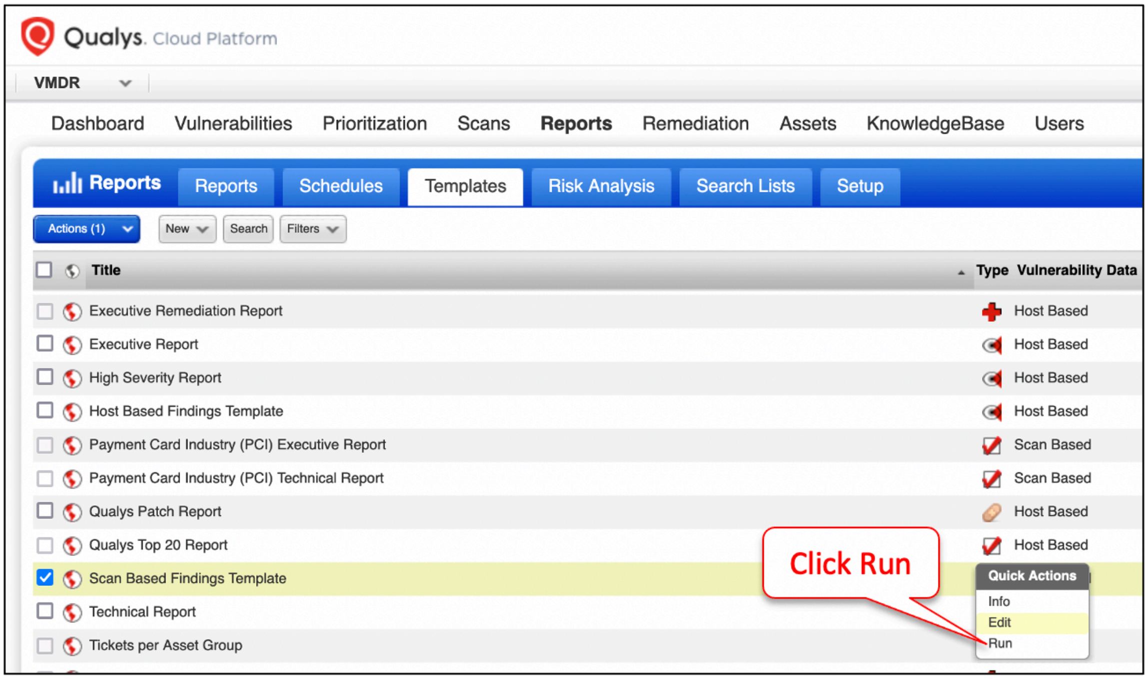
PLAY

Lab: Scan Based Template

https://ior.ad/7Bbk

Create Scan Based Findings Report

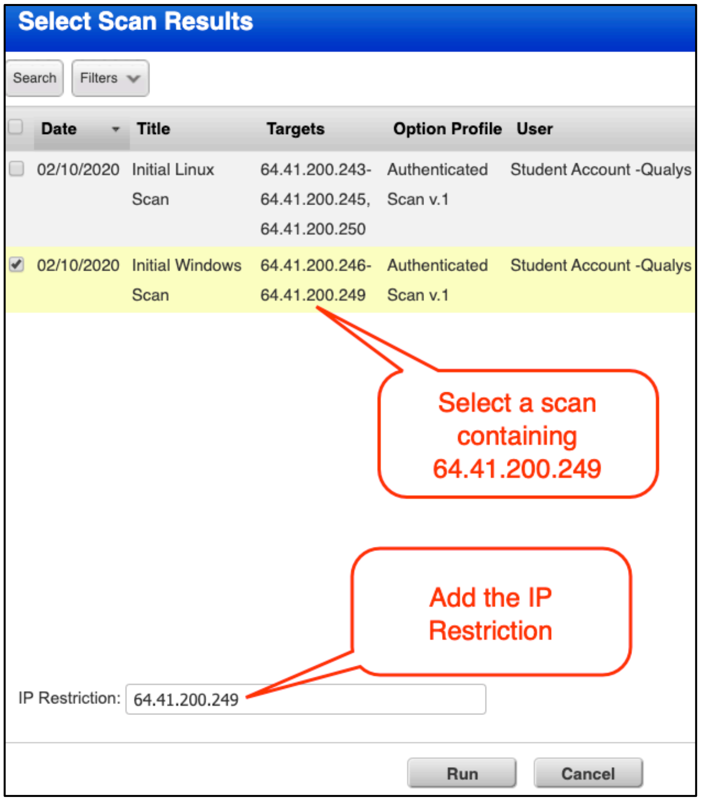
Scan Based Findings have the benefit of building reports that isolate or target a single scan but can also be used to isolate or target a single host.



	Title	Type	Vulnerability Data
□	Executive Remediation Report		Host Based
□	Executive Report		Host Based
□	High Severity Report		Host Based
□	Host Based Findings Template		Host Based
□	Payment Card Industry (PCI) Executive Report		Scan Based
□	Payment Card Industry (PCI) Technical Report		Scan Based
□	Qualys Patch Report		Host Based
□	Qualys Top 20 Report		Host Based
☑	Scan Based Findings Template		
□	Technical Report		
□	Tickets per Asset Group		

Click Run

The “IP Restriction” field allows you to select a specific IP address from the scan targets for reporting.

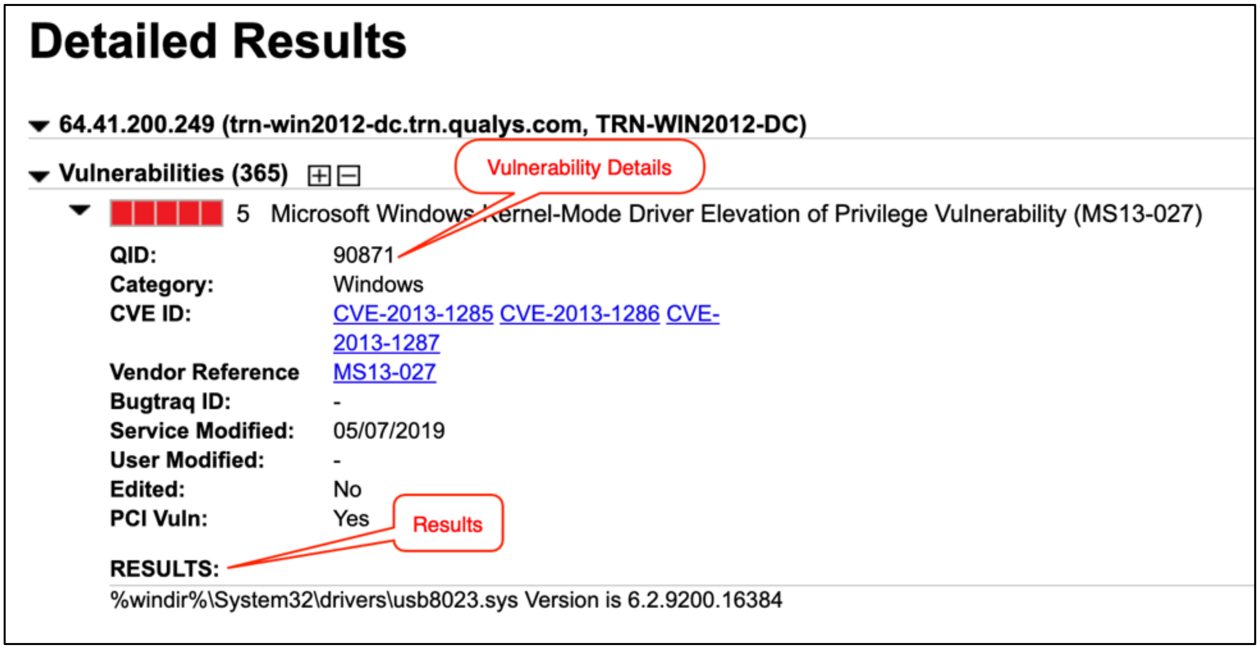


	Date	Title	Targets	Option Profile	User
□	02/10/2020	Initial Linux Scan	64.41.200.243-64.41.200.245, 64.41.200.250	Authenticated Scan v.1	Student Account -Qualys
☑	02/10/2020	Initial Windows Scan	64.41.200.246-64.41.200.249	Authenticated Scan v.1	Student Account -Qualys

Select a scan containing 64.41.200.249

Add the IP Restriction

IP Restriction: 64.41.200.249



Detailed Results

▼ 64.41.200.249 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC)

▼ Vulnerabilities (365) ⊞⊟

▼ 🟥🟥🟥🟥🟥 5 Microsoft Windows Kernel-Mode Driver Elevation of Privilege Vulnerability (MS13-027)

QID:	90871
Category:	Windows
CVE ID:	CVE-2013-1285 CVE-2013-1286 CVE-2013-1287
Vendor Reference	MS13-027
Bugtraq ID:	-
Service Modified:	05/07/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

RESULTS:

```
%windir%\System32\drivers\usb8023.sys Version is 6.2.9200.16384
```

The report gives you the scan results for just the one host you entered. The details you see will depend on the options configured in the Template – this case, Text Summary, Vulnerability Details and Results.

Navigate to the following URL to view the lab tutorial for this topic:

PLAY

Lab: Scan Based Report

https://ior.ad/7Bbs

LAB 8: Report - Display Options (Time: 5 mins)

This lab will now move from the “Findings” options within a Scan Report Template, to the “Display” options. You can use the various display options to add graphics and summary information to your reports, as well as selecting the details that will be provided for each vulnerability.

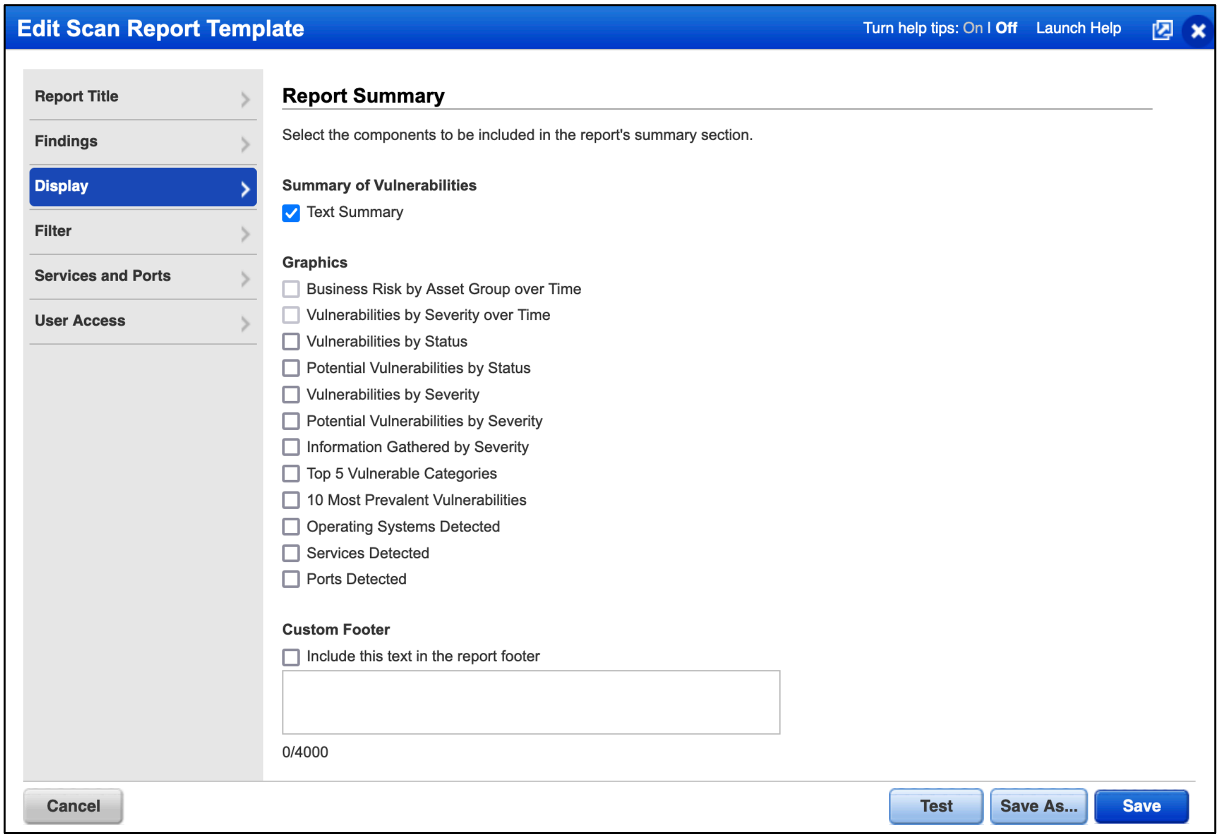
You will typically want to adjust the display options for different user groups within your organization.

Report Summary

The text summary includes the total number of vulnerabilities detected, the overall security risk, and the business risk (for reports sorted by asset group).

Graphics that show data over time (like ‘Business Risk by Asset Group over Time) can be enabled only if “Include Trending” is enabled under the “Findings tab”.

Under Custom Footer you can add required information like a disclosure statement or data classification (e.g. Public, Confidential).



Report Summary

Select the components to be included in the report's summary section.

Summary of Vulnerabilities

☑ Text Summary

Graphics

□ Business Risk by Asset Group over Time
□ Vulnerabilities by Severity over Time
□ Vulnerabilities by Status
□ Potential Vulnerabilities by Status
□ Vulnerabilities by Severity
□ Potential Vulnerabilities by Severity
□ Information Gathered by Severity
□ Top 5 Vulnerable Categories
□ 10 Most Prevalent Vulnerabilities
□ Operating Systems Detected
□ Services Detected
□ Ports Detected

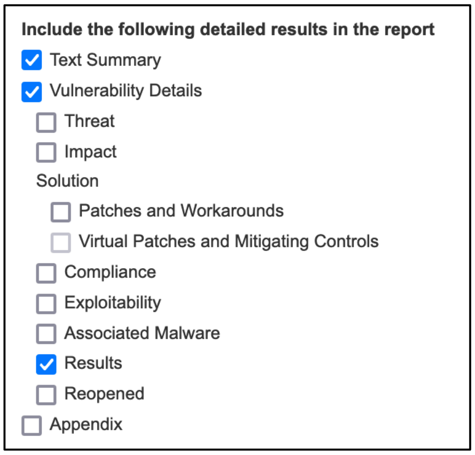
Custom Footer

□ Include this text in the report footer

0/4000

Detailed Results

Vulnerabilities or QIDs include a LOT of information. Checking all boxes under detailed results will increase the amount of detail, as well as the report size and the amount of time required to generate the report. When selecting included details ask: “What does the target audience need to see?” What information is required to meet the objective at hand?

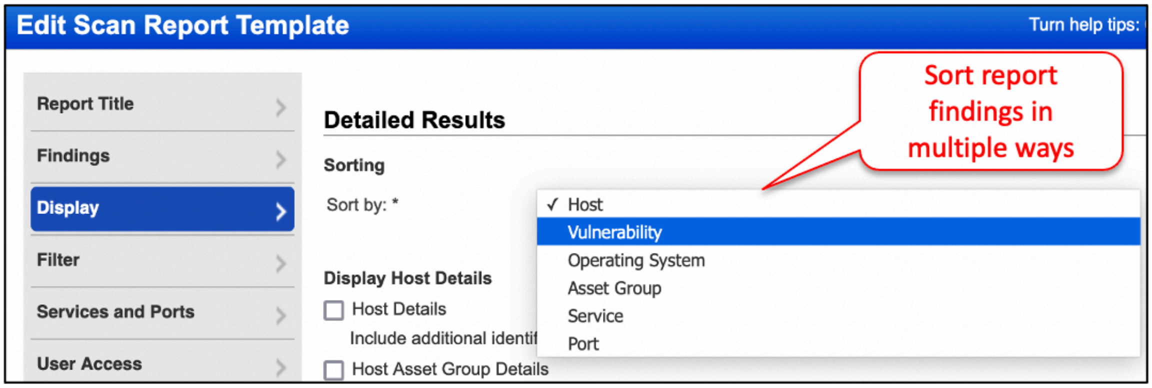


Include the following detailed results in the report

☑ Text Summary
☑ Vulnerability Details
  □ Threat
  □ Impact
  Solution
    □ Patches and Workarounds
    □ Virtual Patches and Mitigating Controls
  □ Compliance
  □ Exploitability
  □ Associated Malware
  ☑ Results
  □ Reopened
□ Appendix

Sorting Data

You can sort report data in multiple ways as indicated below. Sorting by vulnerability is useful when multiple hosts have the same vulnerability findings. Doing so will help reduce the report size as each vulnerability finding will be listed only once and the impacted hosts will be listed underneath the vulnerability.



Edit Scan Report Template

Turn help tips:

Report Title
Findings
Display
Filter
Services and Ports
User Access

Detailed Results

Sorting

Sort by: *

✓ Host
Vulnerability
Operating System
Asset Group
Service
Port

Display Host Details

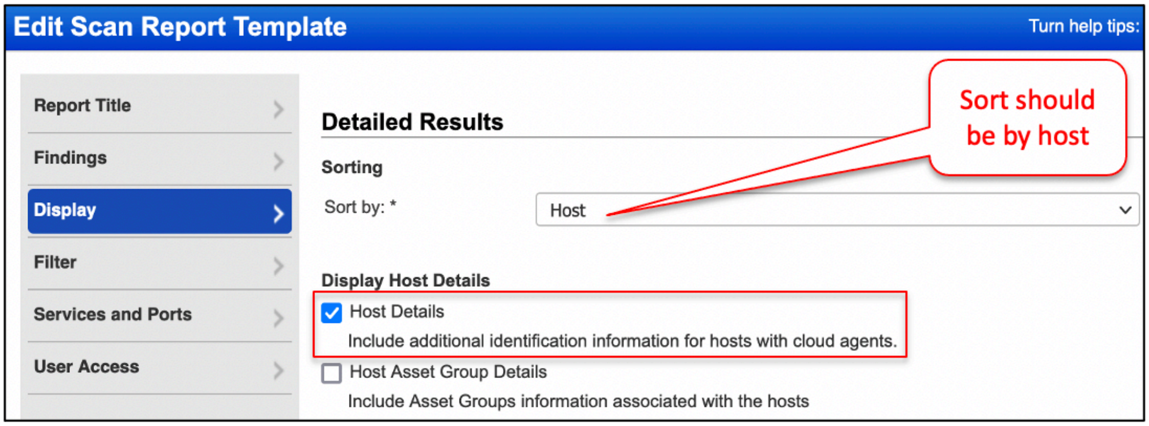
□ Host Details
Include additional identif

□ Host Asset Group Details

Sort report findings in multiple ways

Display Host Details

Checking the "Host Details" check box will include the Qualys Host ID (UUID) in your reports , which is the unique identifier associated with its Cloud Agent host. (to use "Host Details" you must change the "Sort by" field back to the "Host" option).



Edit Scan Report Template

Turn help tips:

Report Title
Findings
Display
Filter
Services and Ports
User Access

Detailed Results

Sorting

Sort by: * Host

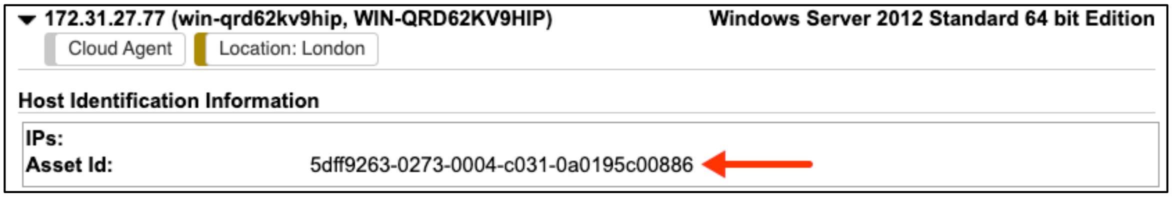
Display Host Details

☑ Host Details
Include additional identification information for hosts with cloud agents.

□ Host Asset Group Details
Include Asset Groups information associated with the hosts

Sort should be by host

The Qualys Host ID for the agent host is visible in the report snippet as illustrated below:



▾ 172.31.27.77 (win-qrd62kv9hip, WIN-QRD62KV9HIP) Windows Server 2012 Standard 64 bit Edition

Cloud Agent | Location: London

Host Identification Information

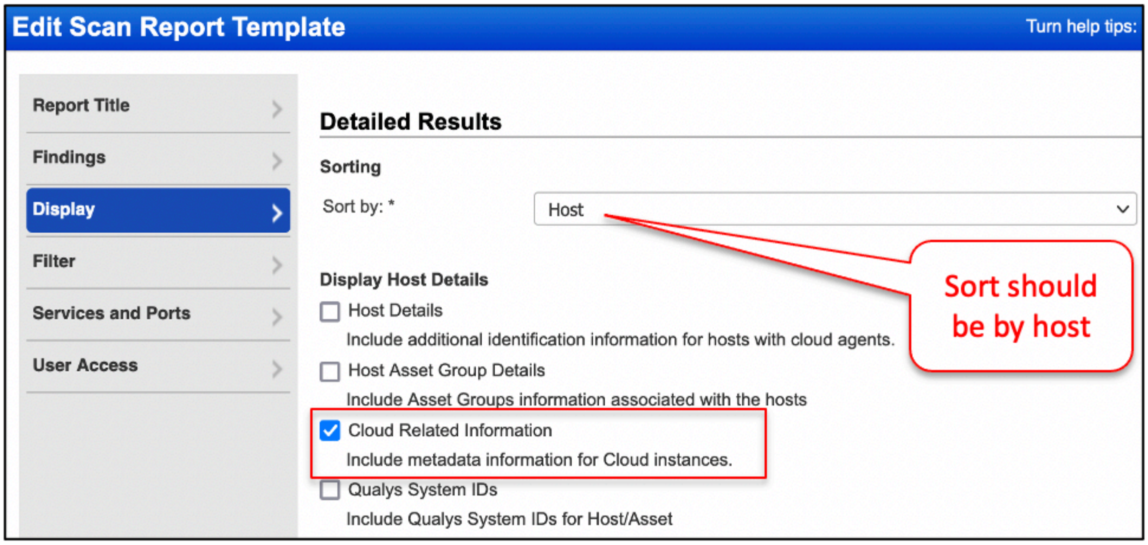
IPs:	
Asset Id:	5dff9263-0273-0004-c031-0a0195c00886

Select the "Qualys System IDs" check box (under Display Host Details) to include host identifiers such as host ID, asset ID in the host-based scan report template.

Cloud Related Information

Select the "Cloud Related Information" check box (under Display Host Details) to include metadata information at the host level for each of your cloud instance in Azure and AWS. You must also select Host Based Findings and Sort by Host in the template.

The EC2 Scanning feature must be enabled for your subscription to use this setting in the report template. Please contact your Technical Account Manager or Support if you would like to have this feature turned on.



Detailed Results

Sorting

Sort by: * Host

Display Host Details

☐ Host Details
Include additional identification information for hosts with cloud agents.

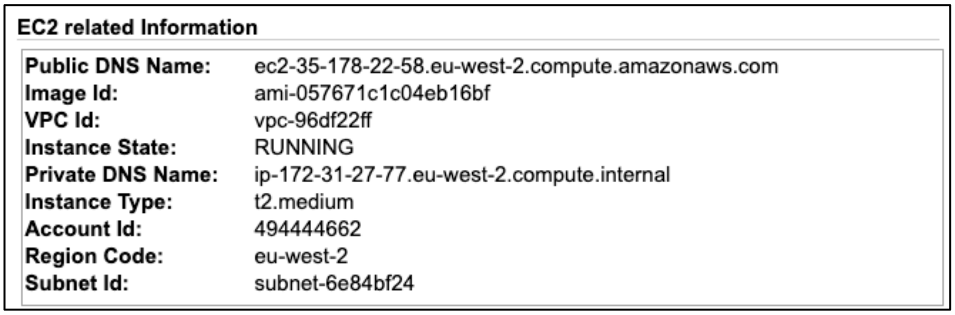
☐ Host Asset Group Details
Include Asset Groups information associated with the hosts

☑ Cloud Related Information
Include metadata information for Cloud instances.

☐ Qualys System IDs
Include Qualys System IDs for Host/Asset

Sort should be by host

The report snippet listed below shows EC2 information as illustrated below:



EC2 related Information

Public DNS Name: ec2-35-178-22-58.eu-west-2.compute.amazonaws.com
Image Id: ami-057671c1c04eb16bf
VPC Id: vpc-96df22ff
Instance State: RUNNING
Private DNS Name: ip-172-31-27-77.eu-west-2.compute.internal
Instance Type: t2.medium
Account Id: 494444662
Region Code: eu-west-2
Subnet Id: subnet-6e84bf24

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Report Template Display Options
https://ior.ad/7BcB

LAB 9: Report - Filter Options (Time: 5 mins)

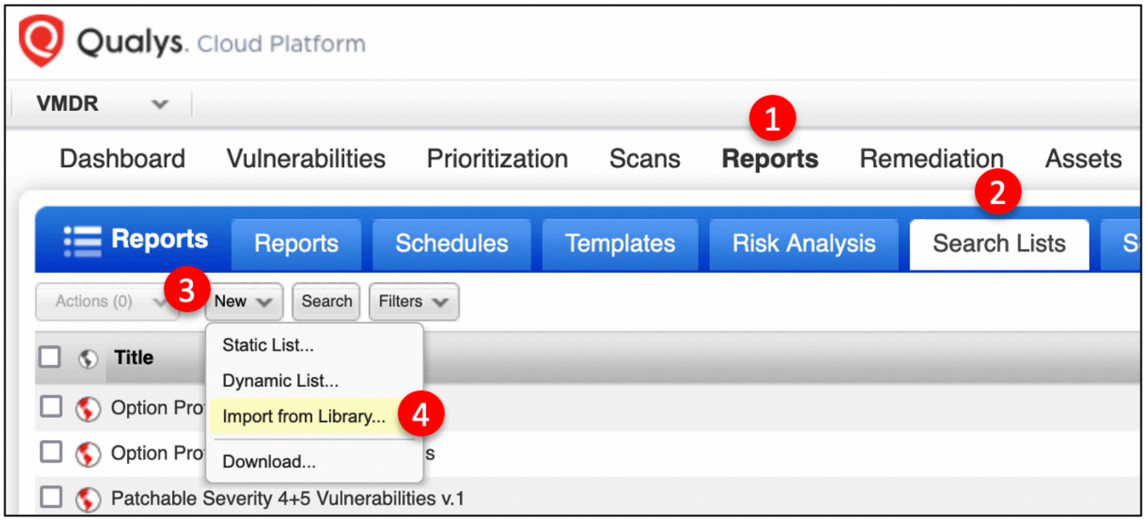
This lab will now explore more functionality of the "Filter" options within a Scan Report Template. You can use the various filter options to narrow down the assets and vulnerabilities on which to create reports.

Selective Vulnerability Reporting

You can create a report template to analyze (filter) specific vulnerabilities.

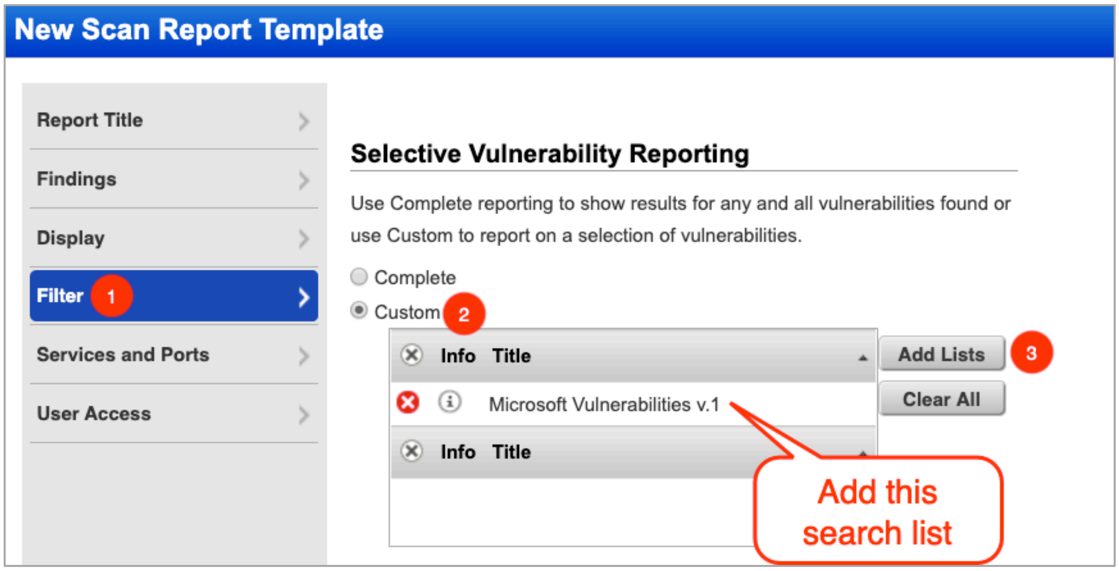
A Search List is one of the most powerful and versatile filtering tools within the Vulnerability Management application. Adding a Search List to a Report Template will allow your reports to focus on specific types and groups of vulnerabilities.

You will find a Search List tab within the "Scans," "Reports," and "KnowledgeBase" sections of the Vulnerability Management application.



Add search lists to your vulnerability scan report template to filter the report to specific QIDs (static search list) or to QIDs that match criteria that you specify (dynamic search list).

In your scan report template, go to the Filter section and select Custom under Selective Vulnerability Reporting. Then add custom search lists from your account or import search lists from our Library.



New Scan Report Template

Selective Vulnerability Reporting

Use Complete reporting to show results for any and all vulnerabilities found or use Custom to report on a selection of vulnerabilities.

○ Complete
● Custom

Info	Title
ⓘ	Microsoft Vulnerabilities v.1

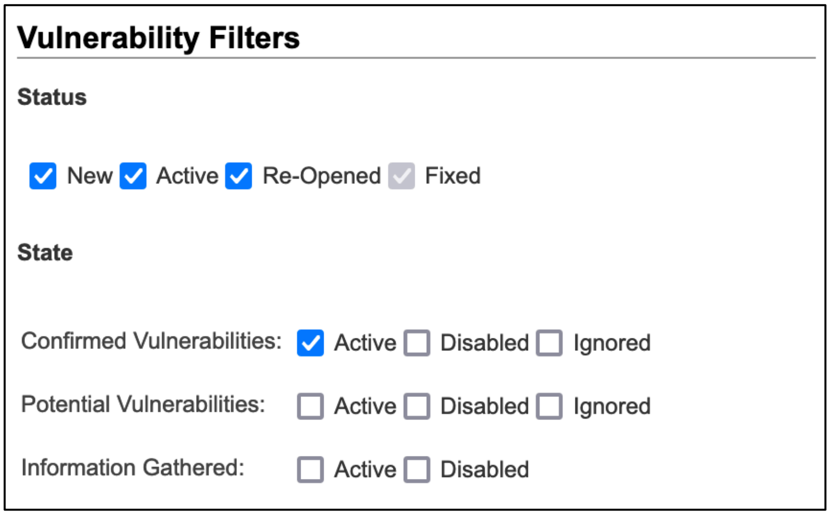
Info	Title

In the above illustration we have added the "Microsoft Vulnerabilities v.1" search list which is imported from the search list library. By adding this search list to the template, your reports will focus only on the confirmed Microsoft Vulnerabilities (instead of all of the vulnerabilities) found on each host.

You can create your own custom Search Lists that allow your reports to focus (filter) on different types of vulnerabilities, severity levels, or any other criteria found within the Search List editor, including vulnerabilities impacted by known threats.

Vulnerability Filters

Vulnerability Filters allows you to define the status of the vulnerabilities you wish to see in the report. You can choose the status (New, Fixed, Re-Opened, Active) to filter the vulnerabilities. These filters are only applicable when Host Based Findings is selected in the template (on the Findings tab).



Vulnerability Filters

Status

☑ New ☑ Active ☑ Re-Opened ☑ Fixed

State

Confirmed Vulnerabilities: ☑ Active □ Disabled □ Ignored

Potential Vulnerabilities: □ Active □ Disabled □ Ignored

Information Gathered: □ Active □ Disabled

The first time a vulnerability is detected on an asset it's status will be new. For any vulnerabilities that have been detected more than once it's status will be active. When a vulnerability is no longer detected then it's status will be fixed. For any vulnerabilities that have been fixed and are rediscovered then the status is re-opened.

Please note that if you want to report on fixed vulnerabilities you need to have the trending option in the findings enabled.

Along with its status, a vulnerability also has a state, with the default state being active. Meaning that it actively scanned for and reported on. A vulnerability can also be disabled via the knowledge base. Meaning it is globally filtered out from all hosts in the scan report

For specific reasons sometimes, a vulnerability may be disabled or ignored for a period of time. If you wish to report on these then you will need to select relevant state option.

An ignored vulnerability is a specific vulnerability that is ignored on a specific asset.

Navigate to the following URL to view the lab tutorial for this topic:

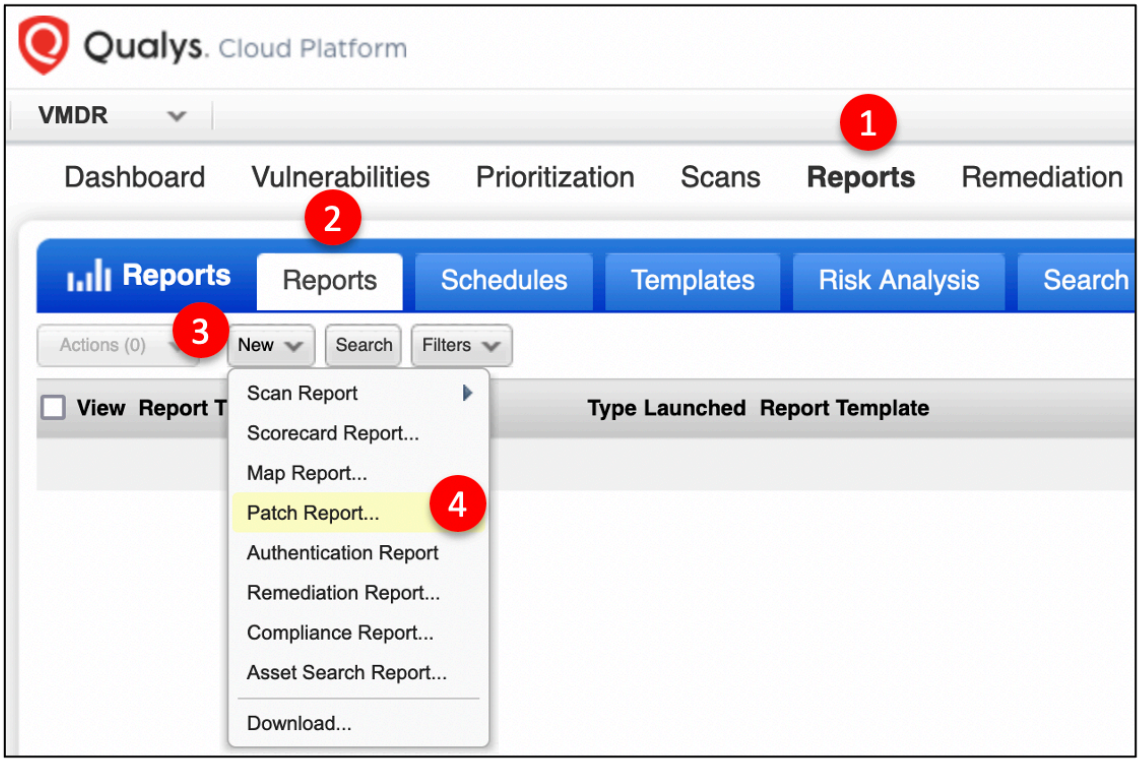
PLAY

Lab: Report Template Filters

https://ior.ad/7Bbx

LAB 10: Patch Report (Time: 5 mins)

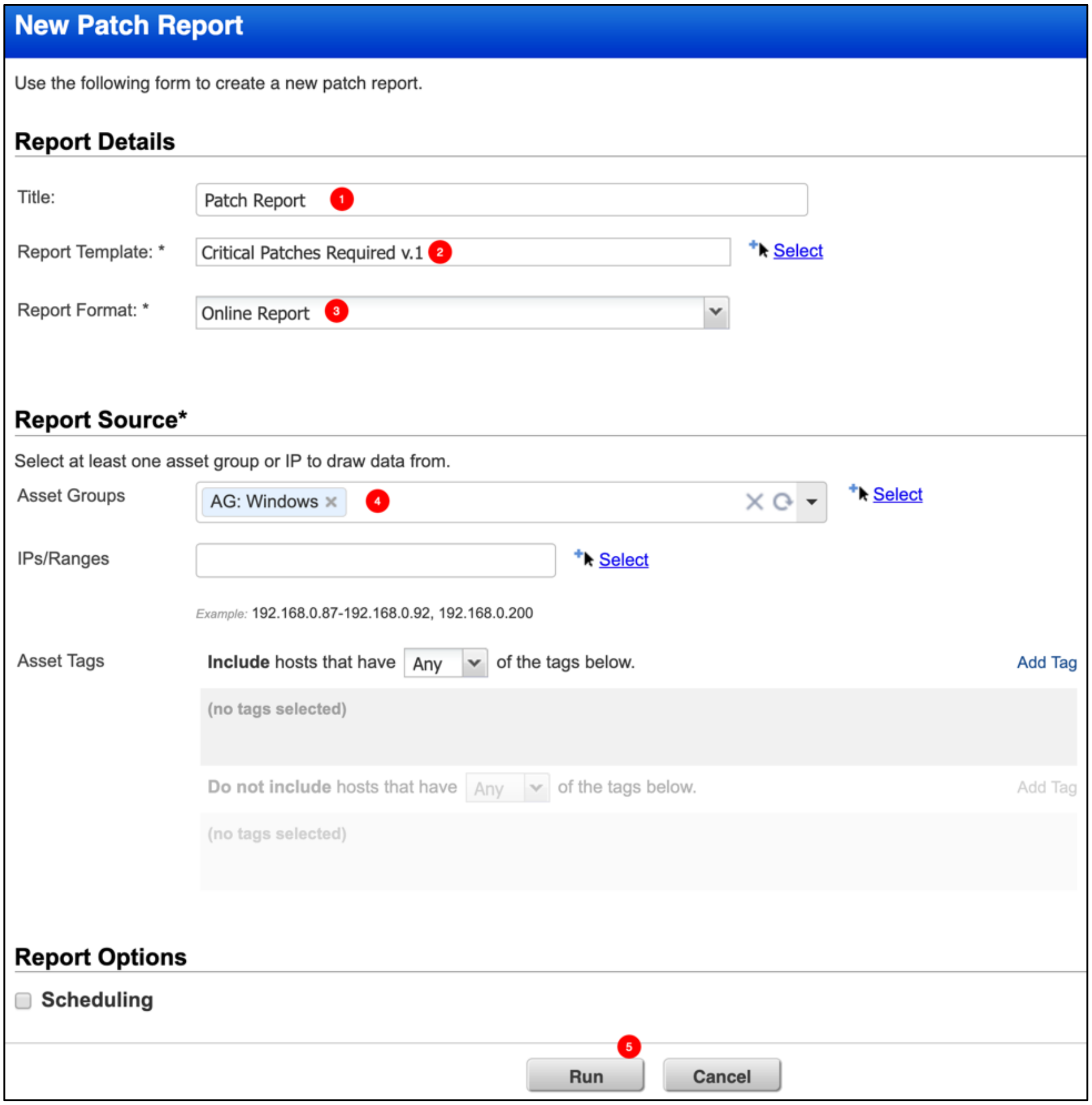
In this section you will use the Patch Report template to create a Patch Report. Patch reports provide current patch information for fixing vulnerabilities and prioritizing remediation tasks. A patch report identifies the most recent fixes for detected vulnerabilities in your account, so you can apply the fewest patches necessary to fix your vulnerabilities. Note that a patch report includes only vulnerabilities that have available patches and excludes vulnerabilities that cannot be patched.



Launch patch reports to find out about the patches you need to apply to fix your current vulnerabilities. You'll be able to use the links in this report to quickly download and install missing patches.

Online Report Format

This report format provides a feature-rich user interface including numerous ways to navigate through your report content. HTML content is displayed in your browser using Ext, a client-side Java framework. A patch report in Online Report format cannot be downloaded to your local filesystem.



New Patch Report

Use the following form to create a new patch report.

Report Details

Title: Patch Report 1

Report Template: * Critical Patches Required v.1 2 Select

Report Format: * Online Report 3

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups AG: Windows × 4 Select

IPs/Ranges Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags **Include** hosts that have Any of the tags below. Add Tag

(no tags selected)

Do not include hosts that have Any of the tags below. Add Tag

(no tags selected)

Report Options

□ Scheduling

5 Run Cancel

The patch report identifies the patches available for current vulnerabilities on selected hosts based on a patch template selected by the user at run time. These are the vulnerabilities detected by the most recent scan of each selected host.

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Patch Report

https://ior.ad/7BcN

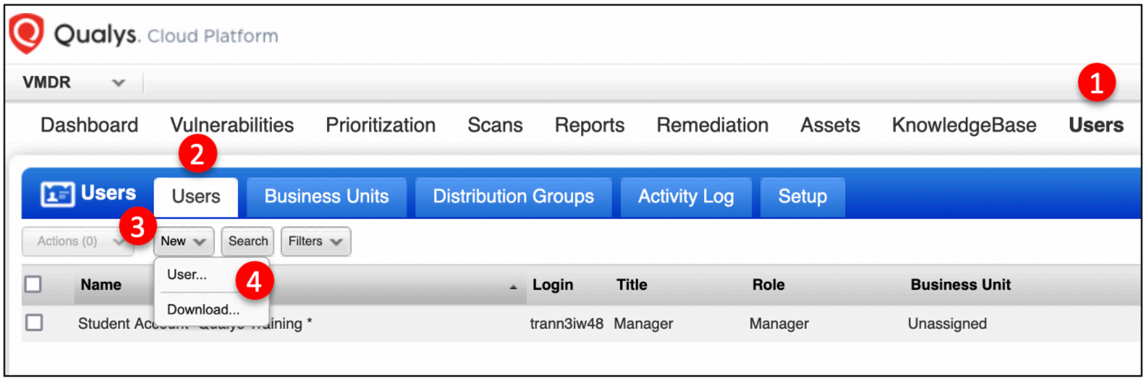
LAB 11: Report Scheduling and Distribution (Time: 10 mins)

You can schedule your reports to run automatically - daily, weekly, monthly. This way you'll get the most up to date vulnerability data with the most accurate trends. Also, you can schedule reports to run at important milestones, like the last day of the quarter, without logging in to do it.

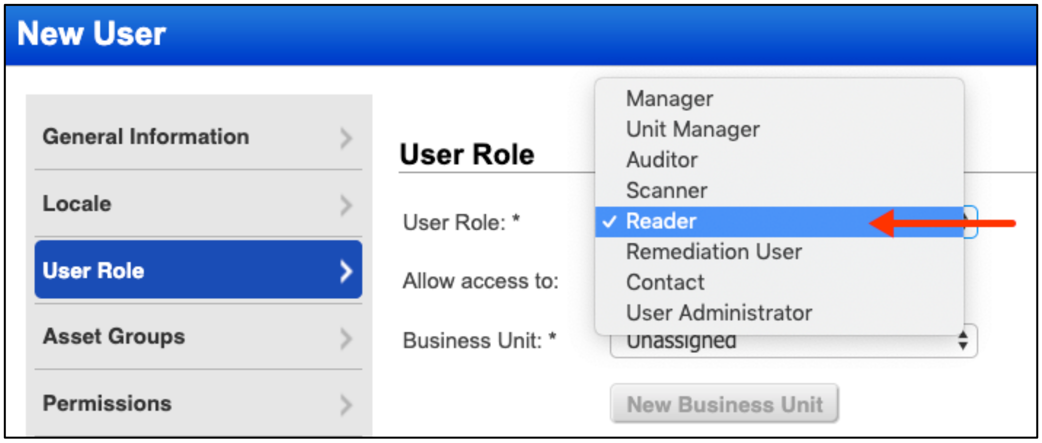
This lab will walk you through the process of creating a user and distributing reports in different ways.

Create a User

Each user is assigned a pre-defined user role (Manager, Unit Manager, Scanner, etc) which determines the actions the user can take. You start by creating a user and assigning the user a role which comes with a basic set of permissions, for example the role Reader allows the user to create reports.



Name	Login	Title	Role	Business Unit
Student Ac… …aining *	trann3iw48	Manager	Manager	Unassigned



User Role: * Reader

Allow access to:

Business Unit: * Unassigned

When you create a new user, the user appears on the user accounts list with a status of "Pending Activation". The user will automatically receive a registration email with a secure one-time-only link to the credentials for their new account and login instructions. The registration email is sent to the email address defined in the user's account. The user's status changes to "Active" after logging in for the first time.

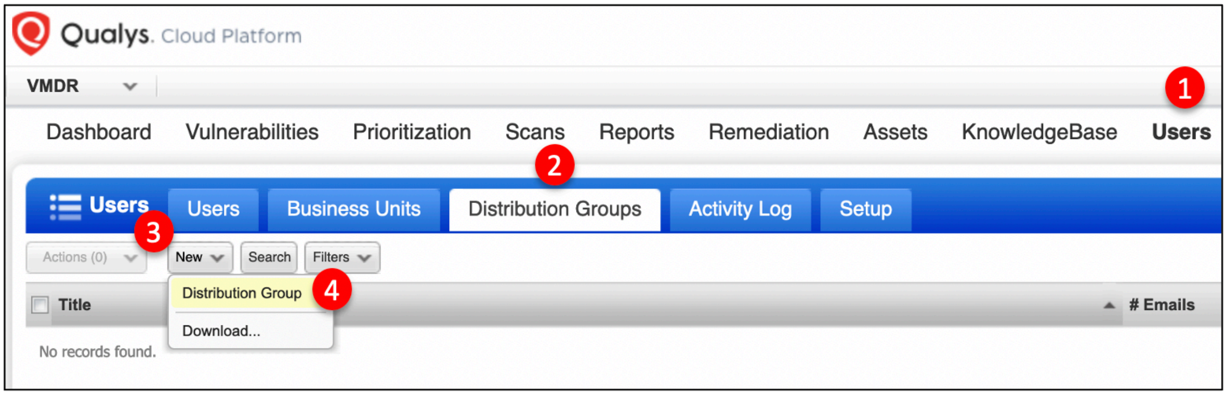
Navigate to the following URL to view the lab tutorial for this topic:

Lab: Create a User

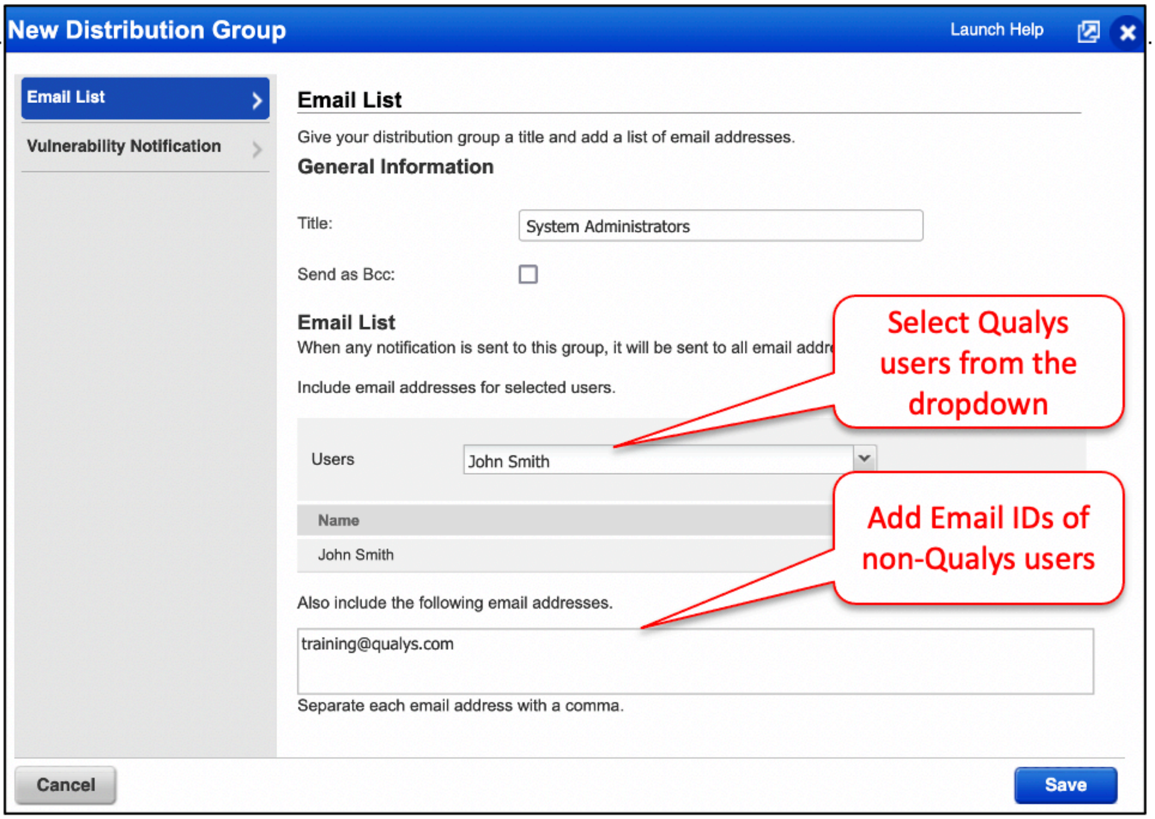
https://ior.ad/7Bdd

Create a Distribution Group

You can have certain email notifications sent to a group of people by setting up distribution groups. You can choose distribution groups for several email notifications, including scan notifications, report notifications and the vulnerability notification.



You can include email addresses for users in the subscription (simply select users from the list) and include email addresses for users outside of the subscription by typing them into the field provided.



Email List

Give your distribution group a title and add a list of email addresses.

General Information

Title: System Administrators

Send as Bcc: □

Email List

When any notification is sent to this group, it will be sent to all email addr

Include email addresses for selected users.

Users: John Smith

Name
John Smith

Also include the following email addresses.

training@qualys.com

Separate each email address with a comma.

Select Qualys users from the dropdown

Add Email IDs of non-Qualys users

Navigate to the following URL to view the lab tutorial for this topic:

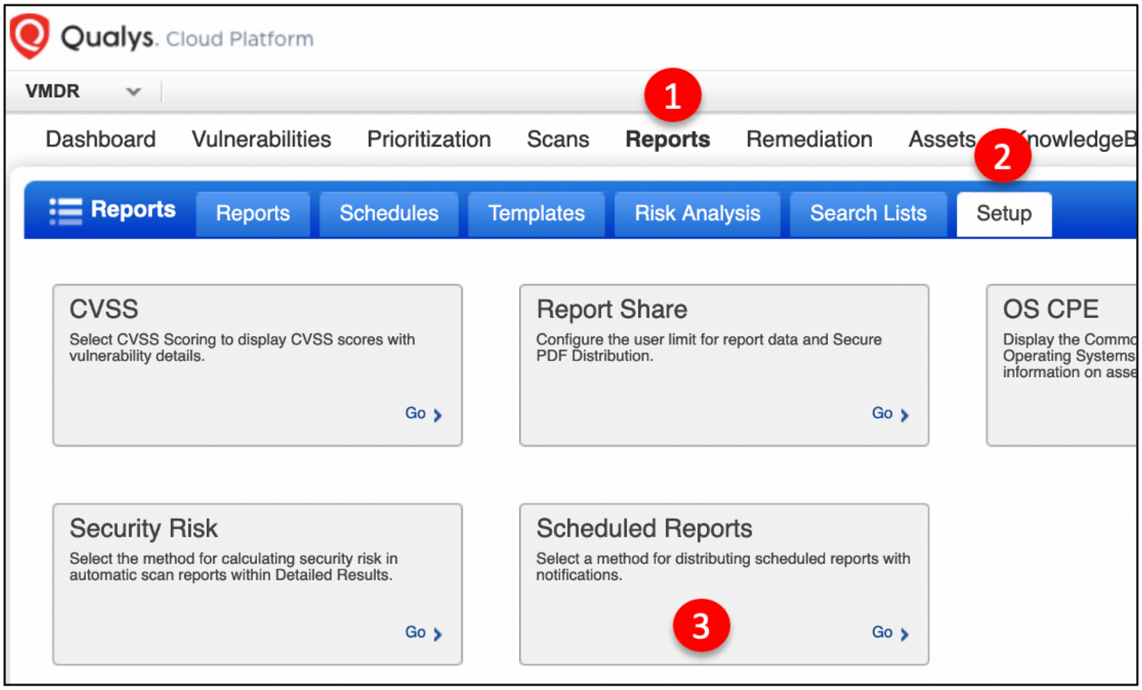
PLAY

Lab: Create a Distribution Group

https://ior.ad/7Bd1

Define Report Distribution Method

You need to configure global settings for the subscription to determine if scheduled reports will be distributed with report notifications, and whether they will be sent as attachments or report links. This configuration is done under Reports-> Setup.



CVSS

Select CVSS Scoring to display CVSS scores with vulnerability details.

Report Share

Configure the user limit for report data and Secure PDF Distribution.

OS CPE

Display the Commo Operating Systems information on asse

Security Risk

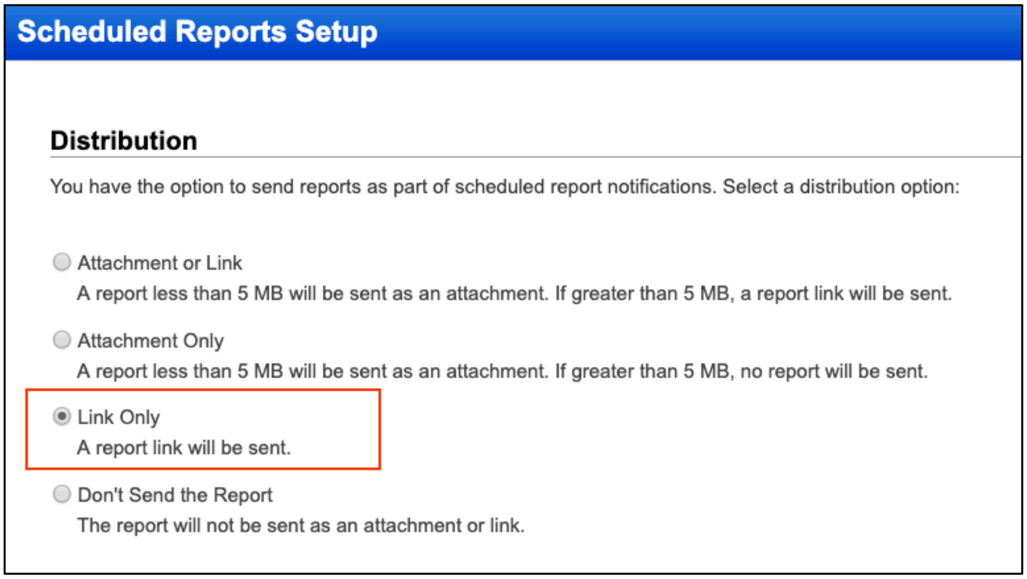
Select the method for calculating security risk in automatic scan reports within Detailed Results.

Scheduled Reports

Select a method for distributing scheduled reports with notifications.

There are four options to distribute scheduled reports:

- **Attachment or Link** - As noted, if the report is under 5 MB, it will be sent as an attachment. If it's over 5 MB, a link will be sent. The person receiving the report does not have to have a Qualys user account, they will still receive the report. Note, when sent as an attachment, a copy of that report (possibly containing host vulnerability information) is on your email server.
- **Attachment Only** - If the report is under 5 MB, it will be sent to the user. Otherwise, the user will have to log in to Qualys. Be sure the users you are distributing the report to *can* log in to the Qualys UI, otherwise you will create a manual process for yourself to get them the report.
- **Link Only** - This is a good way to distribute a report to non-Qualys users. You can send an email to them with a link for them to download the report. It is recommended that you password protect the report you send them.
- **Don't Send the Report** - Only use this if sending the report to people who have a Qualys account. They need to log in to get the report. This makes users authenticate.



Scheduled Reports Setup

Distribution

You have the option to send reports as part of scheduled report notifications. Select a distribution option:

○ Attachment or Link
A report less than 5 MB will be sent as an attachment. If greater than 5 MB, a report link will be sent.

○ Attachment Only
A report less than 5 MB will be sent as an attachment. If greater than 5 MB, no report will be sent.

● Link Only
A report link will be sent.

○ Don't Send the Report
The report will not be sent as an attachment or link.

Note that when a report is sent as a link recipients must download the report from the link as soon as possible as the report is deleted from the report share after 7 days or earlier (if the user share limit reaches the maximum allocated size).

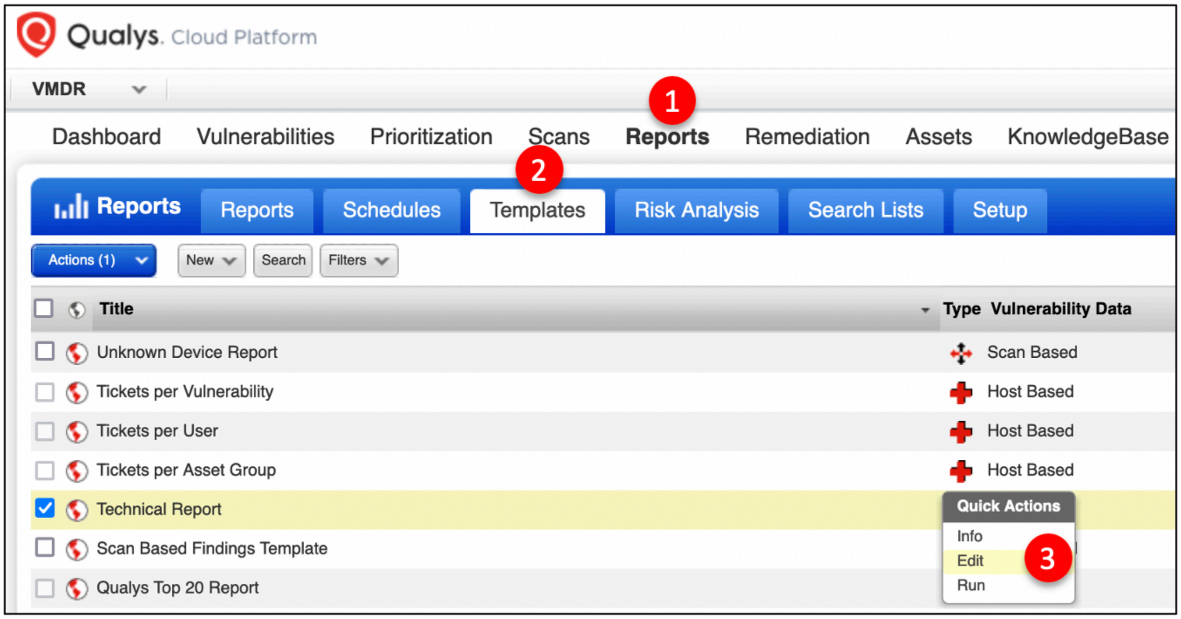
Navigate to the following URL to view the lab tutorial for this topic:

PLAY **Lab**: Report Distribution Setup
https://ior.ad/7Bfa

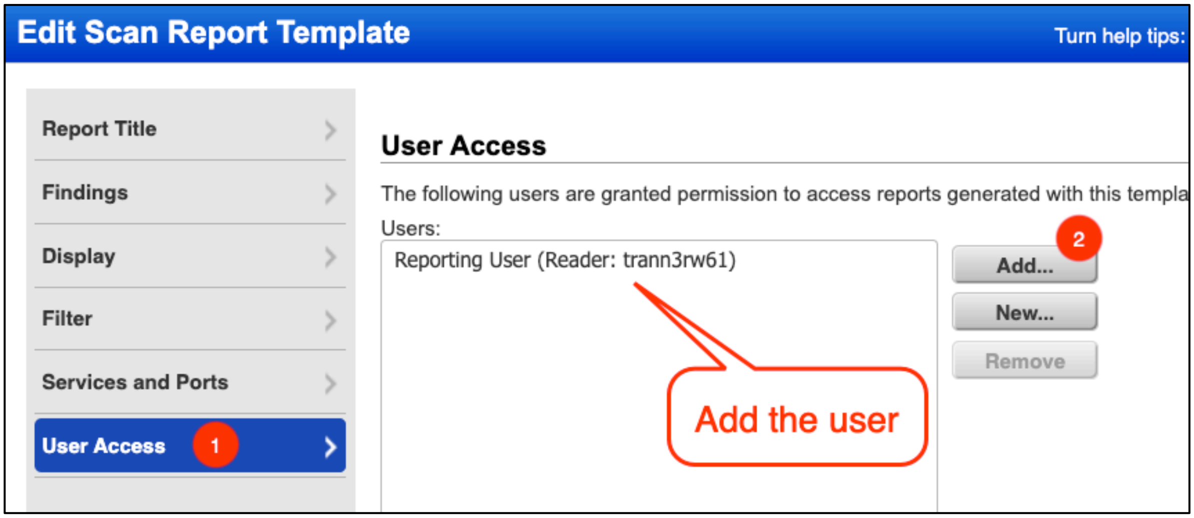
Assign a User to the Template

A good way to build a scalable reporting solution is to assign the right users to the right templates. This ensures a couple things. As a manager user, you can standardize your reporting, meaning you know what data people are using. You'll be able to control who is seeing what.

Assigning users to templates is easy. You'll go to the template, and you will simply find the user who should be able to see the vulnerability data for the assets in this template. This is important, because now, when you schedule a report to run with this template, this user will automatically see it in their account under the reports tab. They will not have to generate the report themselves.



	Title	Type	Vulnerability Data
□	Unknown Device Report		Scan Based
□	Tickets per Vulnerability		Host Based
□	Tickets per User		Host Based
□	Tickets per Asset Group		Host Based
☑	Technical Report		
□	Scan Based Findings Template		
□	Qualys Top 20 Report		



User Access

The following users are granted permission to access reports generated with this templa

Users:

Reporting User (Reader: trann3rw61)

Navigate to the following URL to view the lab tutorial for this topic:

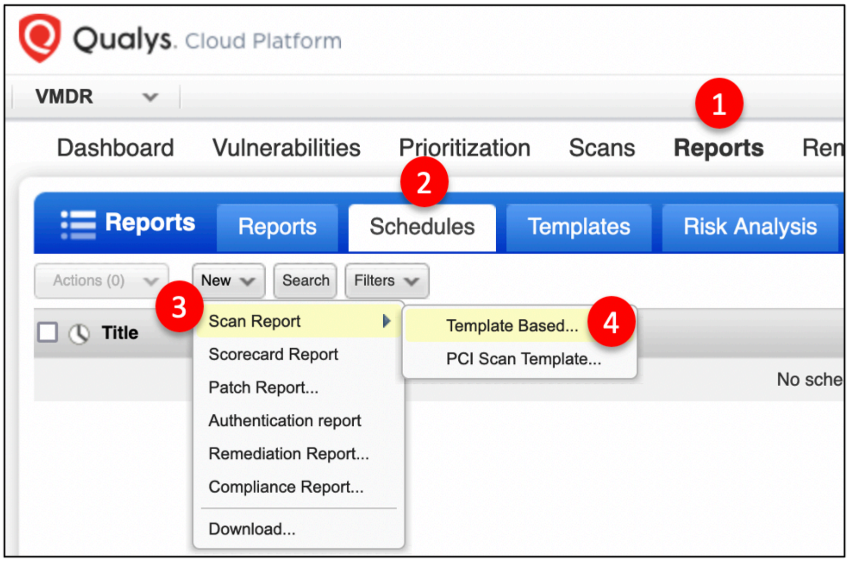
Lab: Add User to a Template

https://ior.ad/7Bfj

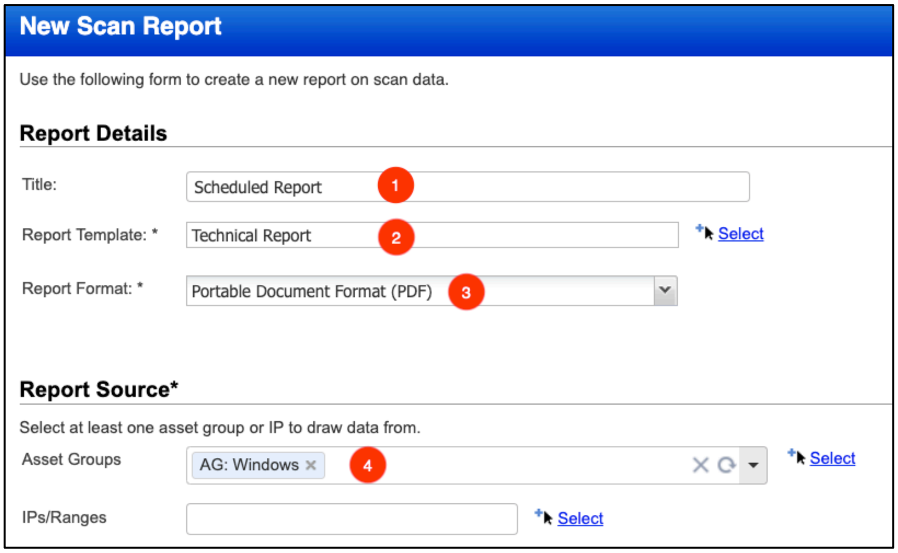
Schedule a Report

You can schedule reports to run automatically at a scheduled time, on a recurring basis. There are several report types that can be scheduled. You can schedule template-based scan reports (set to Auto source selection), scorecard reports, patch reports, template-based compliance reports and remediation reports.

In the example below, a new template-based scan report will be scheduled.



You need to enter report settings such as a template, format, target, etc.



New Scan Report

Use the following form to create a new report on scan data.

Report Details

Title: Scheduled Report (1)

Report Template: * Technical Report (2) Select

Report Format: * Portable Document Format (PDF) (3)

Report Source*

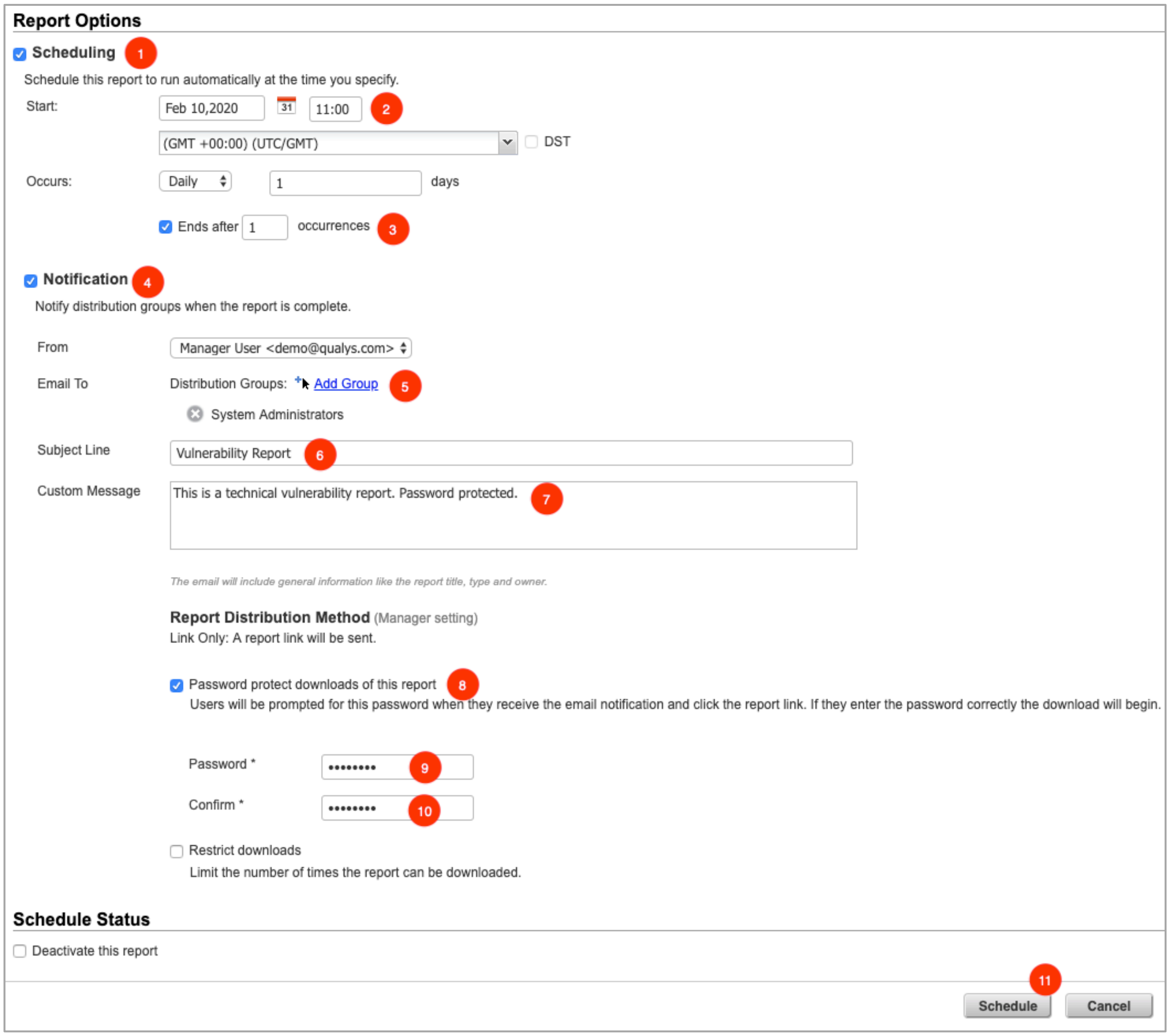
Select at least one asset group or IP to draw data from.

Asset Groups: AG: Windows × (4) Select

IPs/Ranges: Select

Under Scheduling, you'll tell us when and how often your report should run. In this illustration, the report is scheduled to run every day at 11am UTC/GMT.

You can also set options to notify select distribution groups when a report is complete and ready for viewing.



Report Options

☑ **Scheduling** 1

Schedule this report to run automatically at the time you specify.

Start: Feb 10,2020 | 11:00 2

(GMT +00:00) (UTC/GMT) □ DST

Occurs: Daily | 1 days

☑ Ends after 1 occurrences 3

☑ **Notification** 4

Notify distribution groups when the report is complete.

From: Manager User <demo@qualys.com>

Email To: Distribution Groups: Add Group 5

System Administrators

Subject Line: Vulnerability Report 6

Custom Message: This is a technical vulnerability report. Password protected. 7

The email will include general information like the report title, type and owner.

Report Distribution Method (Manager setting)

Link Only: A report link will be sent.

☑ Password protect downloads of this report 8

Users will be prompted for this password when they receive the email notification and click the report link. If they enter the password correctly the download will begin.

Password *: •••••••• 9

Confirm *: •••••••• 10

□ Restrict downloads

Limit the number of times the report can be downloaded.

Schedule Status

□ Deactivate this report

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Schedule a Report

https://ior.ad/7BfQ

LAB 12: Ignore Vulnerabilities (Time: 15 mins)

Remediation policies are commonly used to assign detected vulnerabilities to remediation owners for mitigation. However, these policies can also be used to automatically ignore vulnerabilities and hence accept risk for vulnerabilities you do not plan to address as per your exception handling criteria.

Let's consider the following scenario where you are required to create a Remediation policy to ignore specific vulnerabilities automatically as per the criteria set up by your security team:
"My organization recently implemented a policy to disable Adobe Flash Player in all web browsers and applications company-wide. And so the security team has decided that all existing Adobe Flash Player vulnerabilities need to be ignored as accepted risk without any time limits for expiry, on all assets. Also, all such ignored vulnerabilities must be assigned to the asset owner for review and tracking. How can we accomplish this?"

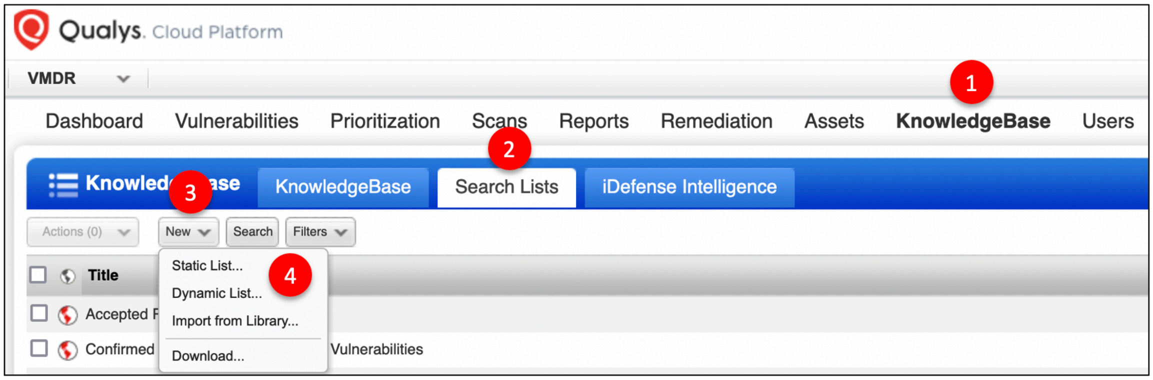
This tutorial will walk you walks you through the steps of creating a Remediation policy to ignore vulnerabilities for the above scenario.

You can also ignore vulnerabilities manually using scan reports (HTML format) based on host-based findings and from host information available through asset search results.

Create Search List

You must configure search lists (static and/or dynamic) to filter specific vulnerabilities matching your exception handling criteria and use these search lists in the remediation policy.

A Dynamic Search list is automatically updated by the Qualys service in conjunction with updates to the Qualys KnowledgeBase. A Static Search list does not receive automatic updates. Typically, static lists are used to collect vulnerabilities that do not have a common criterion.



Accepted F

Confirmed Vulnerabilities

Navigate to the following URL to view the lab tutorial for this topic:

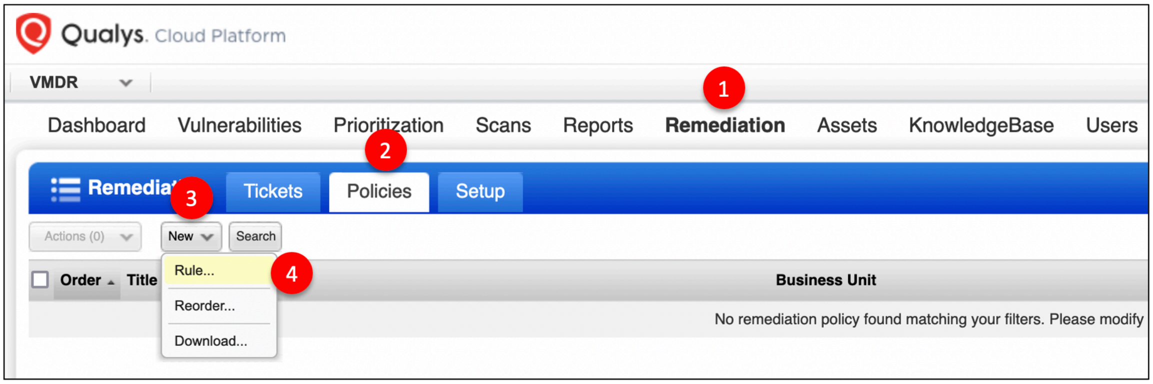
Lab: Create Search List

https://ior.ad/7Bro

Create Remediation Policy

Remediation policy rules enable you to automate the process for ignoring (and hence accepting risk) for select vulnerabilities. Automation minimizes the risk of missing service level agreements and makes it easier to manage multiple items, because you are eliminating manual intervention.

You can set up a rule for vulnerabilities that can't be remediated or the ones that need to be deferred for a specific period, by identifying the impacted vulnerabilities through a search list (static or dynamic). This way you can automate the process to ignore select vulnerabilities.



No remediation policy found matching your filters. Please modify

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Create remediation Policy

https://ior.ad/7Brx

Relaunch a Scan

An additional vulnerability scan is required, to see the results of the Remediation Policy you just created.

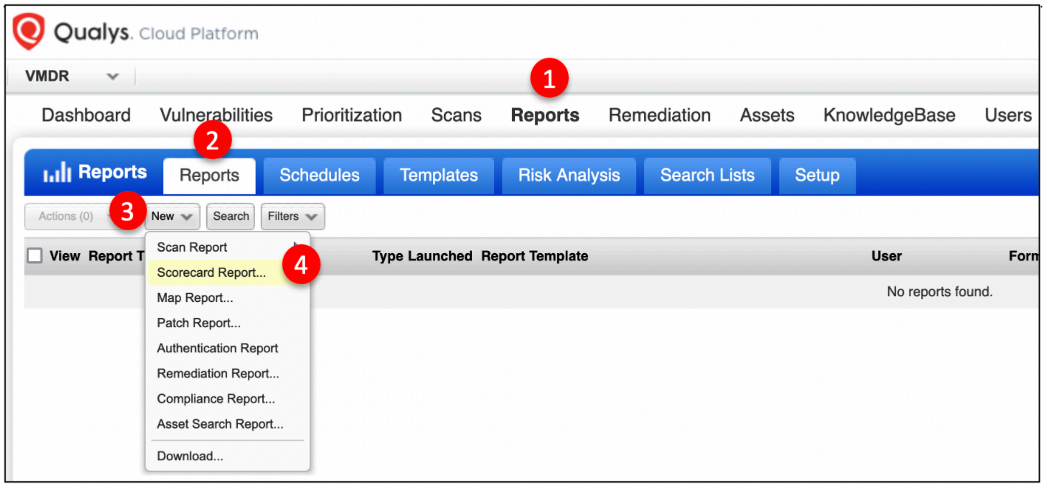
Navigate to the following URL to view the lab tutorial for this topic:

Lab: Run a Scan Job

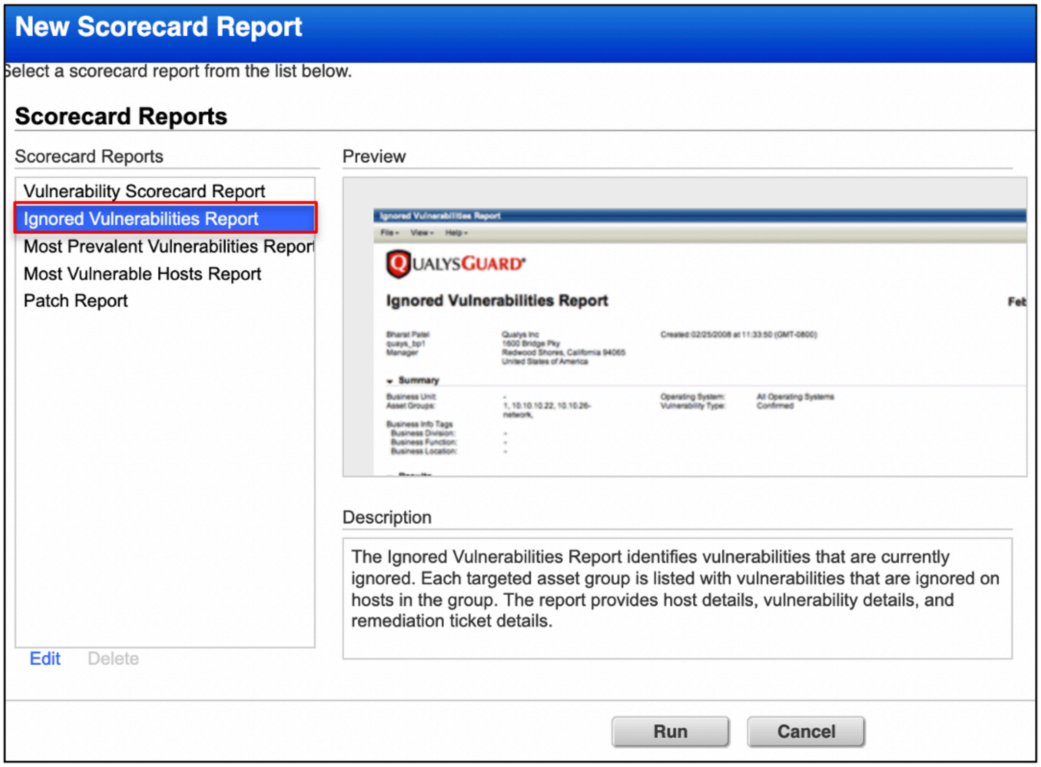
https://ior.ad/7BrF

Monitor Ignored Vulnerabilities

You can track ignored vulnerabilities by using the **Ignored Vulnerabilities** report. You can also use dashboard widgets to track ignored vulnerabilities and also enable trending to track these vulnerabilities over time.



No reports found.



New Scorecard Report

Select a scorecard report from the list below.

Scorecard Reports

Scorecard Reports

- Vulnerability Scorecard Report
- Ignored Vulnerabilities Report
- Most Prevalent Vulnerabilities Report
- Most Vulnerable Hosts Report
- Patch Report

Edit Delete

Preview

Ignored Vulnerabilities Report

File ▾ View ▾ Help ▾

QUALYSGUARD®

Ignored Vulnerabilities Report

Feb

Bharat Patel
qualys_bp1
Manager

Qualys Inc
1600 Bridge Pky
Redwood Shores, California 94065
United States of America

Created 02/25/2008 at 11:33:50 (GMT-0800)

▾ Summary

Business Unit: -
Asset Groups: 1, 10.10.10.22, 10.10.26-network,

Operating System: All Operating Systems
Vulnerability Type: Confirmed

Business Info Tags
Business Division: -
Business Function: -
Business Location: -

Description

The Ignored Vulnerabilities Report identifies vulnerabilities that are currently ignored. Each targeted asset group is listed with vulnerabilities that are ignored on hosts in the group. The report provides host details, vulnerability details, and remediation ticket details.

Navigate to the following URL to view the lab tutorial for this topic:

PLAY

Lab: Ignored Vulnerabilities Report

https://ior.ad/7BrJ

LAB 13: Map a Widget to a Report Template (Time: 10 mins)

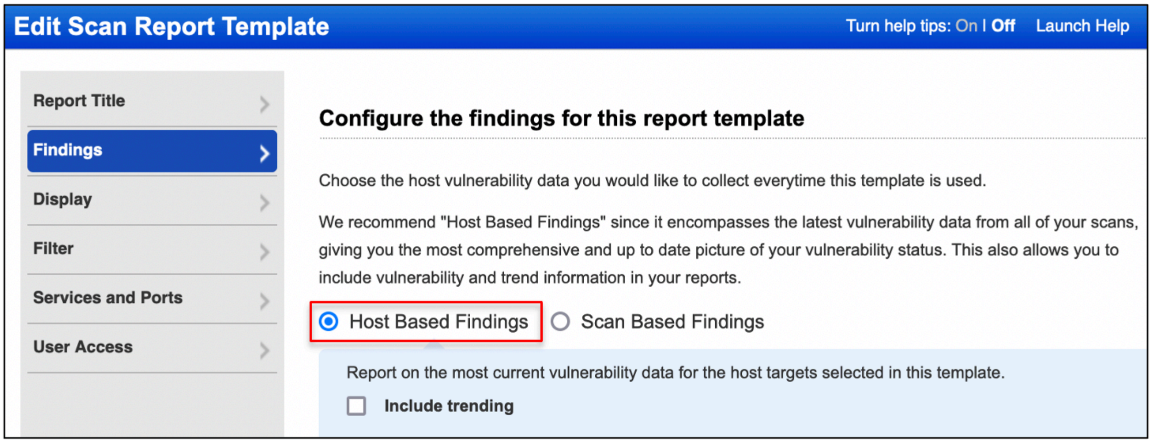
You may want to create dashboard widgets mapped to a report template for better data visualization. This lab activity helps you understand how some of the report template settings\fields map to VM query tokens and widget preferences.

Reviewing your report template filters and making certain that the corresponding widget query tokens and settings are mapped 1 to 1, ensures that your report counts will match your dashboard counts.

So let’s say you have an existing scan report template that creates a report based on the criteria "Confirmed and Patchable and Severity 3 to 5 Vulnerabilities”. And you are tasked with creating a dashboard widget that maps to this report template.

Let’s start by understanding the existing report template configuration.

In this instance, the template used for the report is configured as a Host Based Findings template and does not include trending.



Configure the findings for this report template

Choose the host vulnerability data you would like to collect everytime this template is used.

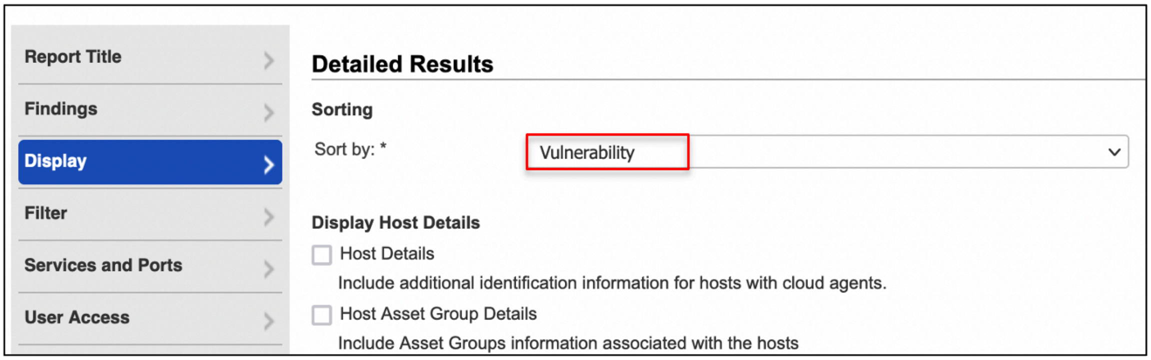
We recommend "Host Based Findings" since it encompasses the latest vulnerability data from all of your scans, giving you the most comprehensive and up to date picture of your vulnerability status. This also allows you to include vulnerability and trend information in your reports.

● Host Based Findings ○ Scan Based Findings

Report on the most current vulnerability data for the host targets selected in this template.

□ Include trending

Under Display, you can see that the report is set to sort results by Vulnerability.



Detailed Results

Sorting

Sort by: * Vulnerability

Display Host Details

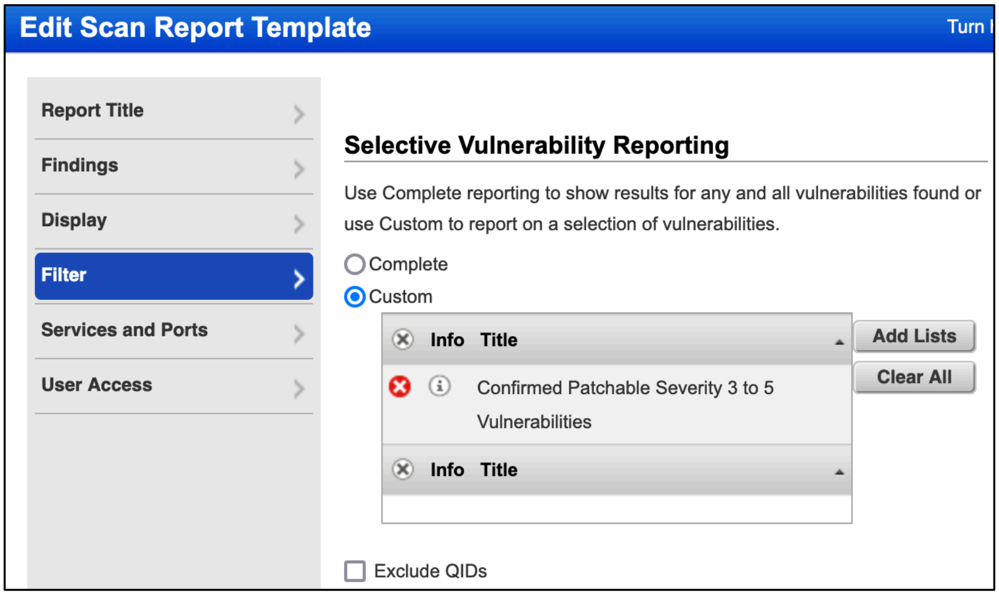
□ Host Details

Include additional identification information for hosts with cloud agents.

□ Host Asset Group Details

Include Asset Groups information associated with the hosts

Under Filter settings, a search list referenced as a vulnerability filter.



Edit Scan Report Template

Selective Vulnerability Reporting

Use Complete reporting to show results for any and all vulnerabilities found or use Custom to report on a selection of vulnerabilities.

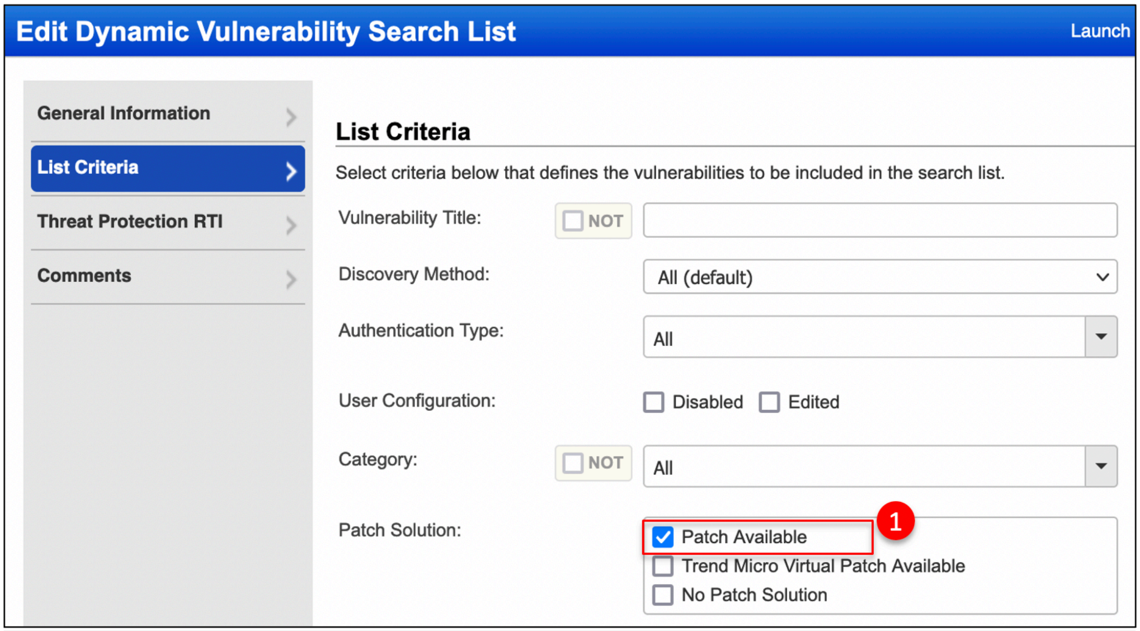
○ Complete

● Custom

Confirmed Patchable Severity 3 to 5 Vulnerabilities

□ Exclude QIDs

The search list referenced in the existing report template is configured to only include patchable and confirmed severity 3, 4 and 5 types of vulnerabilities as illustrated below:



List Criteria

Select criteria below that defines the vulnerabilities to be included in the search list.

Vulnerability Title: □ NOT

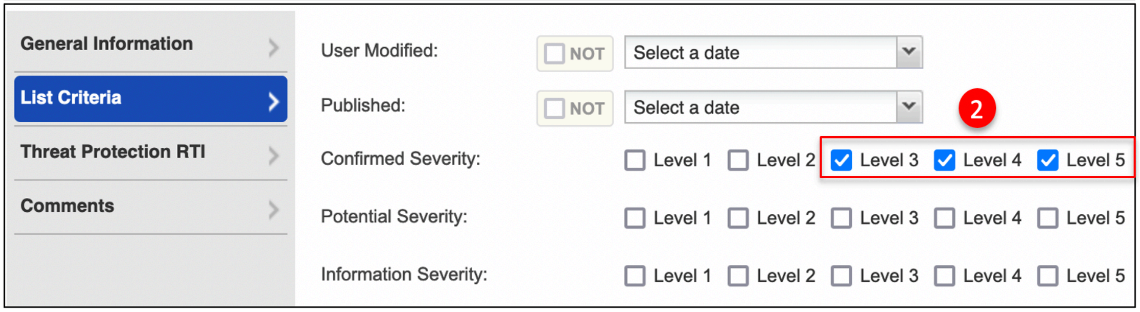
Discovery Method: All (default)

Authentication Type: All

User Configuration: □ Disabled □ Edited

Category: □ NOT All

Patch Solution: ☑ Patch Available □ Trend Micro Virtual Patch Available □ No Patch Solution



User Modified: □ NOT Select a date

Published: □ NOT Select a date

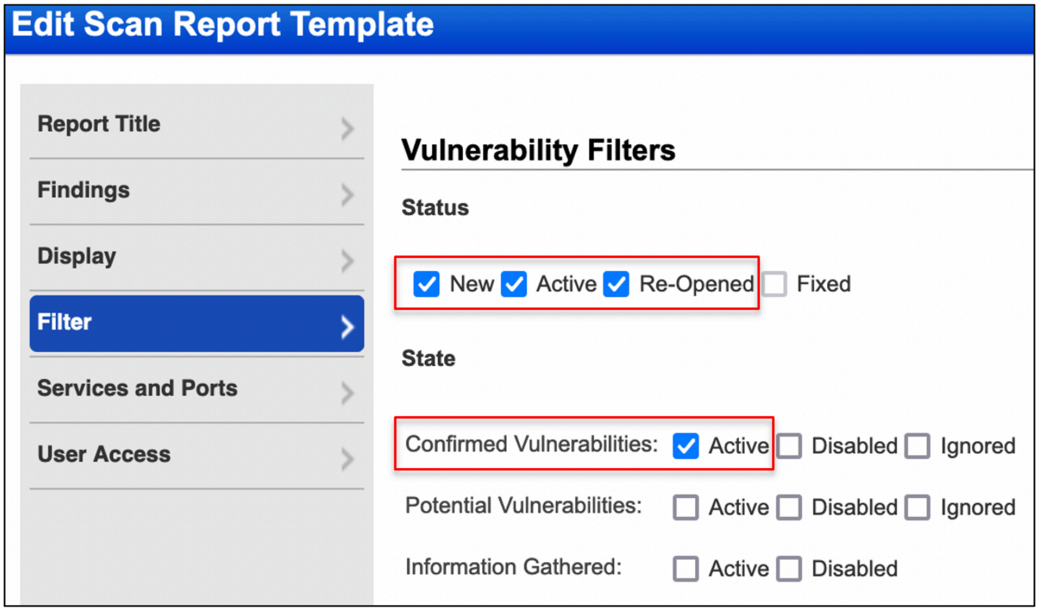
Confirmed Severity: □ Level 1 □ Level 2 ☑ Level 3 ☑ Level 4 ☑ Level 5

Potential Severity: □ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Level 5

Information Severity: □ Level 1 □ Level 2 □ Level 3 □ Level 4 □ Level 5

Further down in the report template, you can see that the report will only include New, Active and Re-opened vulnerabilities. Fixed vulnerabilities are excluded.

Also, only Confirmed, Active vulnerabilities are included. Any Disabled, Ignored vulnerabilities and Information Gathering related QIDs are excluded as illustrated below.



Edit Scan Report Template

- Report Title
- Findings
- Display
- Filter
- Services and Ports
- User Access

Vulnerability Filters

Status

☑ New ☑ Active ☑ Re-Opened □ Fixed

State

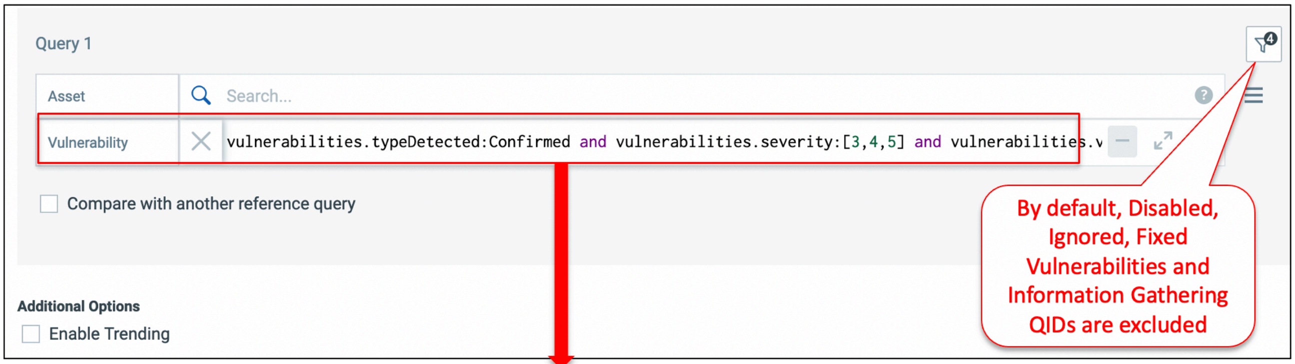
Confirmed Vulnerabilities: ☑ Active □ Disabled □ Ignored

Potential Vulnerabilities: □ Active □ Disabled □ Ignored

Information Gathered: □ Active □ Disabled

Now let’s look at the Widget configuration.

The query used in the widget will filter confirmed, patchable, severity 3,4 and 5 vulnerabilities. Also Disabled, Ignored, Fixed vulnerabilities and Information Gathering QIDs will be excluded from the widget count.



Query 1

Asset | Search...

Vulnerability | `vulnerabilities.typeDetected:Confirmed and vulnerabilities.severity:[3,4,5] and vulnerabilities.v`

□ Compare with another reference query

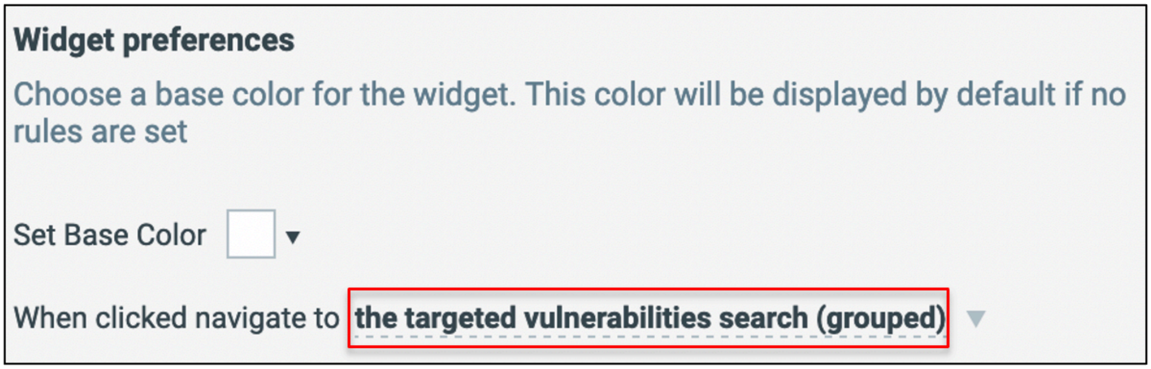
Additional Options

□ Enable Trending

By default, Disabled, Ignored, Fixed Vulnerabilities and Information Gathering QIDs are excluded

```
vulnerabilities.typeDetected:Confirmed and vulnerabilities.severity:[3,4,5] and vulnerabilities.vulnerability.patchAvailable:TRUE
```

Under Widget preferences, you can configure how results are displayed when you click on the widget count. In this instance, you will see the results grouped by Vulnerability as illustrated below.



Widget preferences

Choose a base color for the widget. This color will be displayed by default if no rules are set

Set Base Color □ ▼

When clicked navigate to **the targeted vulnerabilities search (grouped)** ▼

Navigate to the following URL to view the lab tutorial for this topic:

Lab: Map a Widget to a Report Template

https://ior.ad/7BsQ

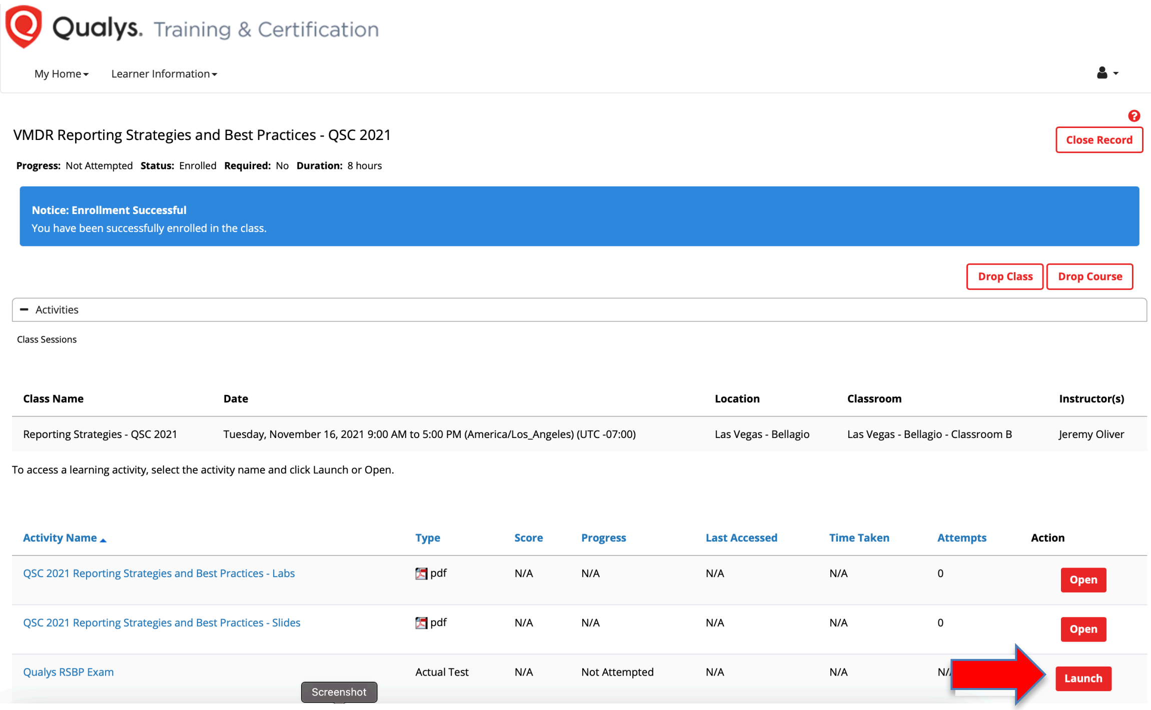
Certification Exam

Participants in this training course have the option to take the Certification Exam. This exam is provided through our Learning Management System (https://qualys.com/learning). To take the exam, candidates will need a “learner” account.

If you would like to take the exam, but do not already have a “learner” account, click the “Request a new account” link (above), from the “Qualys Training & Certification” login page (https://qualys.com/learning).
Once you have created a “learner” account (and for those who already have an account), click the following link to access the QSC 2021 course page:
https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237831

Click the “Enroll” button (lower-right corner).

After successfully completing the course enrollment, click the “Launch” button, for the Exam.



VMDR Reporting Strategies and Best Practices - QSC 2021

Progress: Not Attempted **Status:** Enrolled **Required:** No **Duration:** 8 hours

Notice: Enrollment Successful
You have been successfully enrolled in the class.

Class Sessions

Class Name	Date	Location	Classroom	Instructor(s)
Reporting Strategies - QSC 2021	Tuesday, November 16, 2021 9:00 AM to 5:00 PM (America/Los_Angeles) (UTC -07:00)	Las Vegas - Bellagio	Las Vegas - Bellagio - Classroom B	Jeremy Oliver

To access a learning activity, select the activity name and click Launch or Open.

Activity Name ▲	Type	Score	Progress	Last Accessed	Time Taken	Attempts	Action
QSC 2021 Reporting Strategies and Best Practices - Labs	pdf	N/A	N/A	N/A	N/A	0	Open
QSC 2021 Reporting Strategies and Best Practices - Slides	pdf	N/A	N/A	N/A	N/A	0	Open
Qualys RSBP Exam	Actual Test	N/A	Not Attempted	N/A	N/A	N/	Launch

Each candidate is provided five attempts to pass the exam. You may use the course presentation slides and lab tutorial supplement to help you answer the exam questions.

With a passing score of 75% (or greater), click the “Print Certificate” button to download and print your course exam certificate.

Course Survey and Trial Account

Please lets us know what you think about the QSC 2021 training course.
Survey - https://forms.office.com/r/rsy0Aja6Xz

Would you like a trial account to practice and experiment with the lessons and topics provided in this course?
Link to 30-day Trial - https://www.qualys.com/free-trial/